AWS Cloud WANを使用したセキュアなグローバルネットワーク構築方法

Cloud WAN ＋SASE連携

藤井 拓

Snr. Solutions Architect Network Specialist

2026/3/6

自己紹介

名前：藤井 拓（ふじい たく）

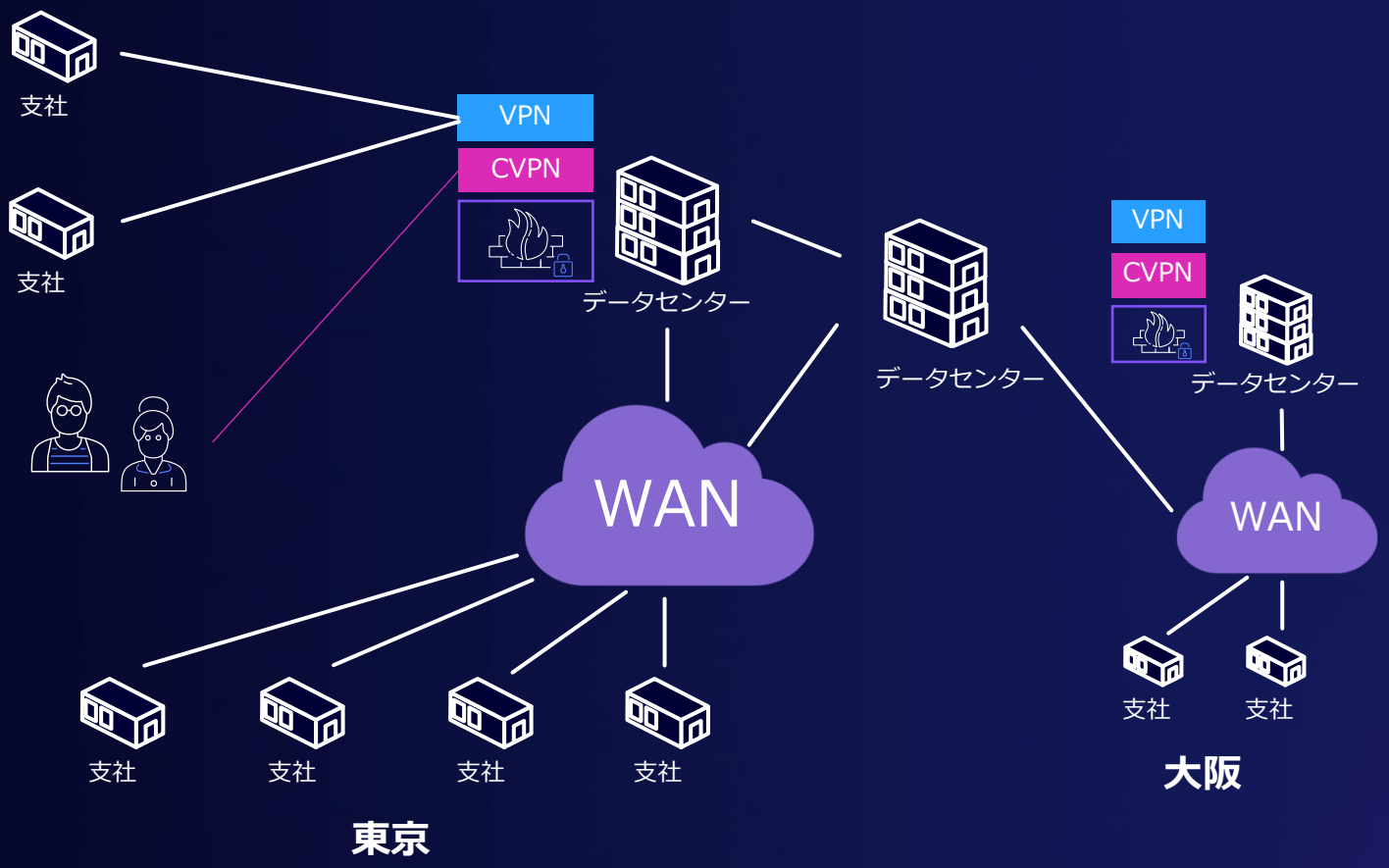
所属：アマゾン ウェブ サービス ジャパン合同会社
　　シニアネットワークソリューションアーキテクト

経歴：前職は外資系ネットワーク機器メーカにてネットワーク機器に関わる
　　プリセールスSEを長年担当

好きなAWSサービス： AWS Transit Gateway, AWS Gateway Load Balancer, AWS Cloud WAN

WANとは

エンタープライズWAN



接続形態

- キャリア網、VPN、Client VPN

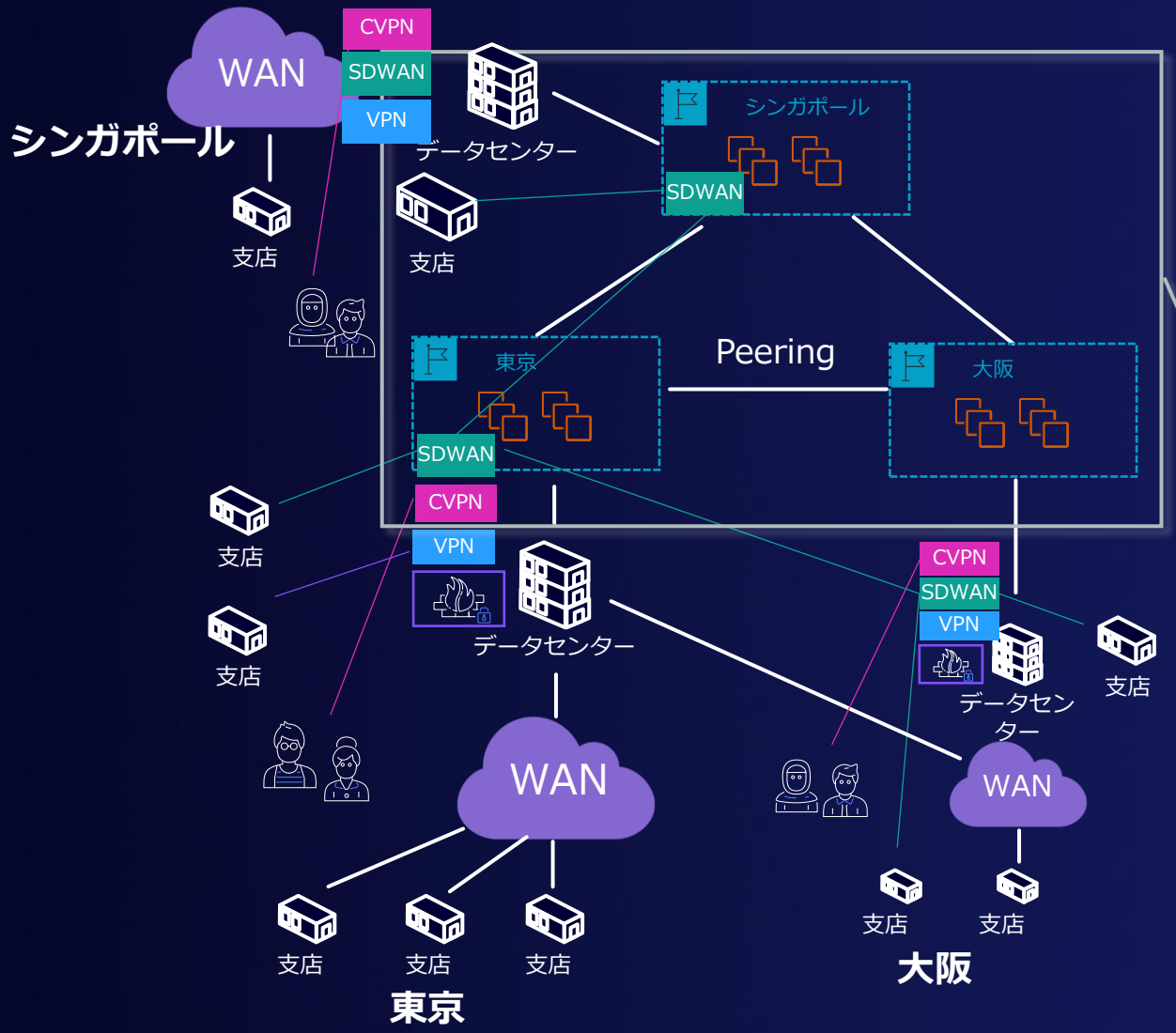
トラフィックフロー

- オフィス拠点間
- オフィス拠点⇔データセンター間
- リモートユーザ⇔データセンター間

課題

- ネットワーク肥大化によるポリシー管理
- 拠点追加時のリードタイム
- 新たに海外拠点追加する際のリードタイムはさらに伸びる

エンタープライズWAN（クラウド接続追加）



追加される接続形態

- クラウド接続、SD-WAN

追加されるトラフィックフロー

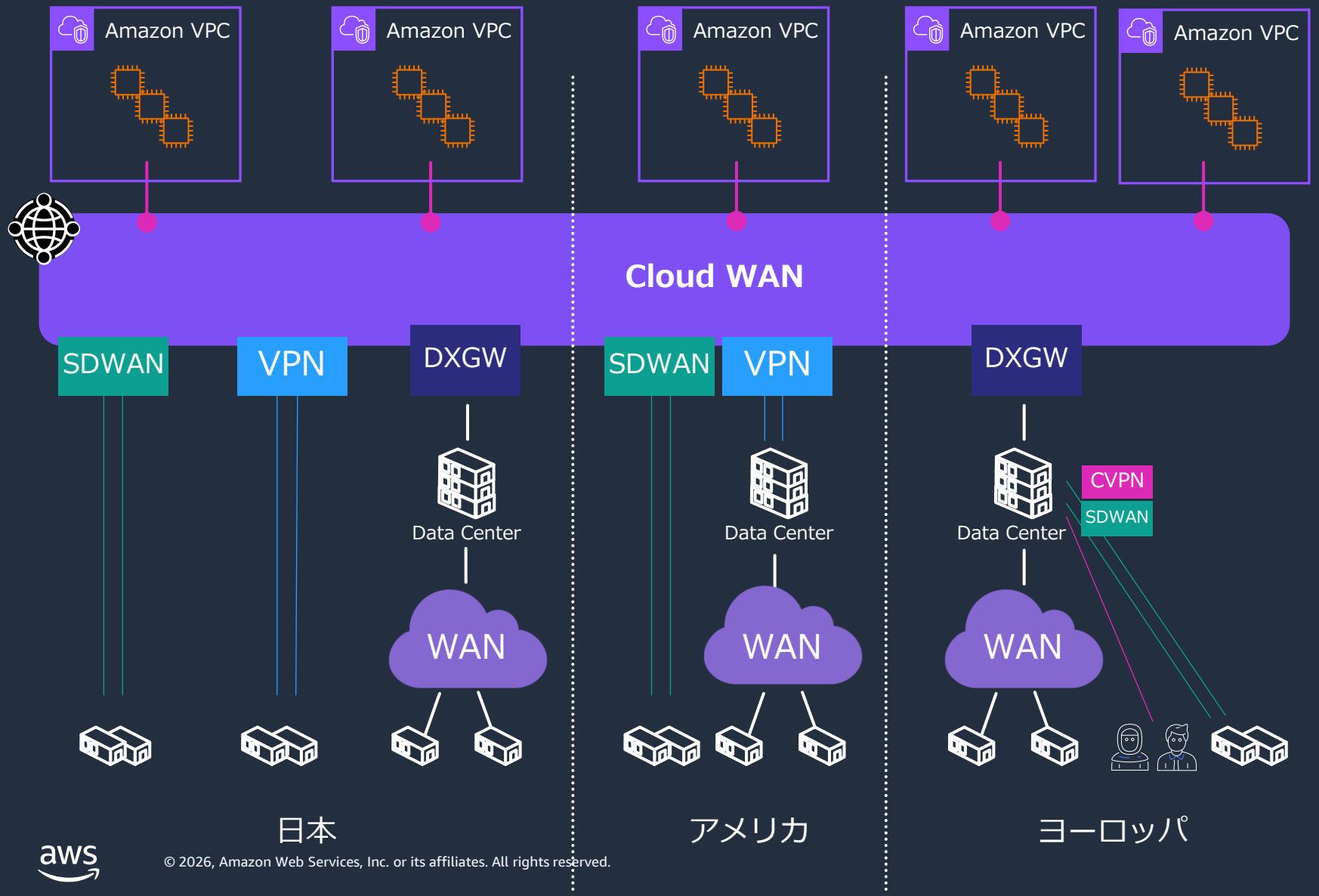
- オンプレミス拠点⇔クラウド
- リモートユーザ⇔クラウド
- クラウドリージョン間の通信
  ⇒SD-WANなどの拠点間通信もクラウド内のバックボーンを通過する場合もある。

課題（将来）

- グローバルネットワークの要件変更対応の迅速化及びポリシー管理
- 新たに国内外の拠点追加する際のリードタイムをより迅速化

AWS Cloud WANとは

Cloud WAN



グローバルネットワーク

リージョンを跨いだネットワーク接続性を提供

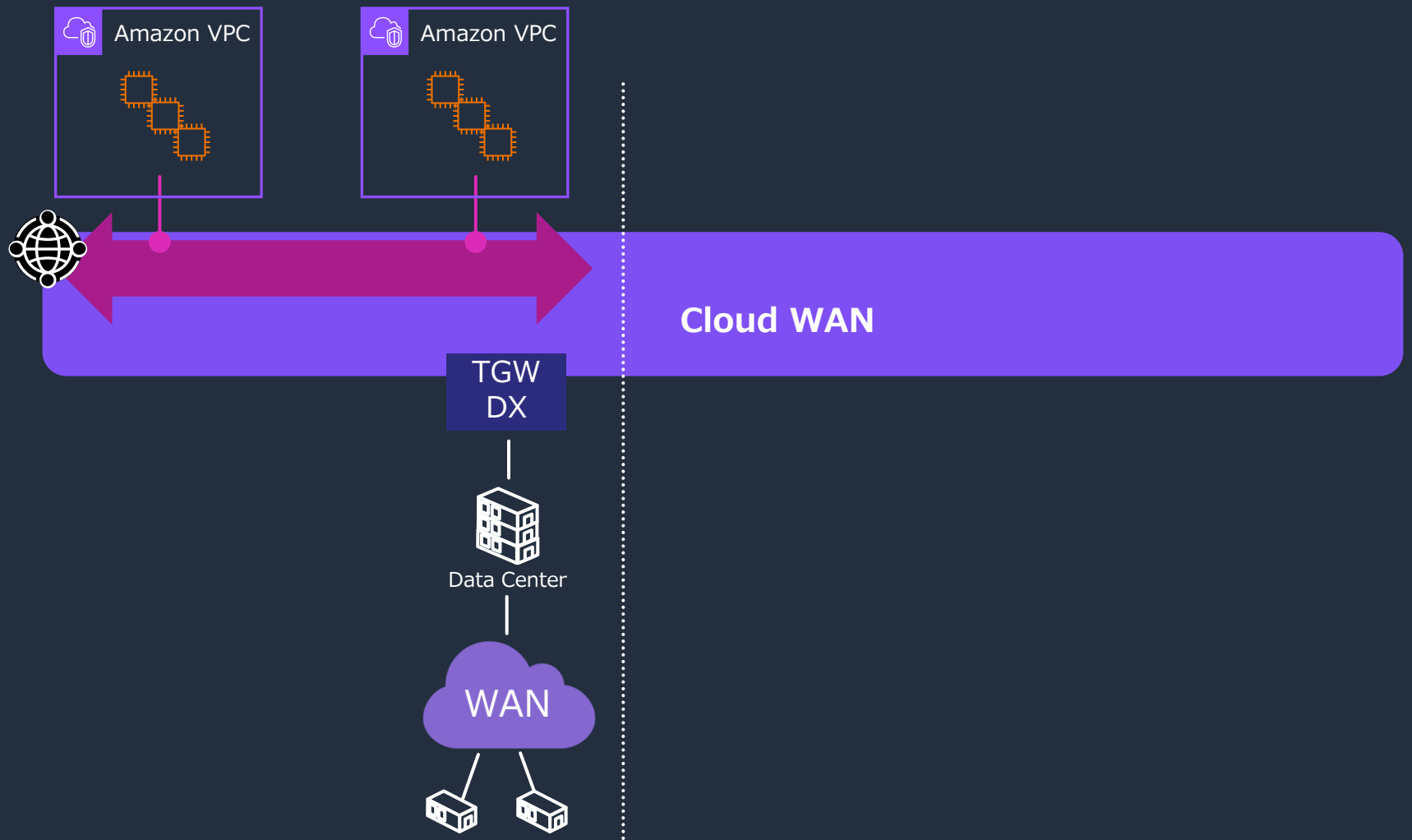
一元管理

ルーティング情報
ネットワークポリシー
日常業務の自動化

アタッチメント

VPCs
VPNs
SD-WAN(TGW Connect)
Transit Gateway RTBs

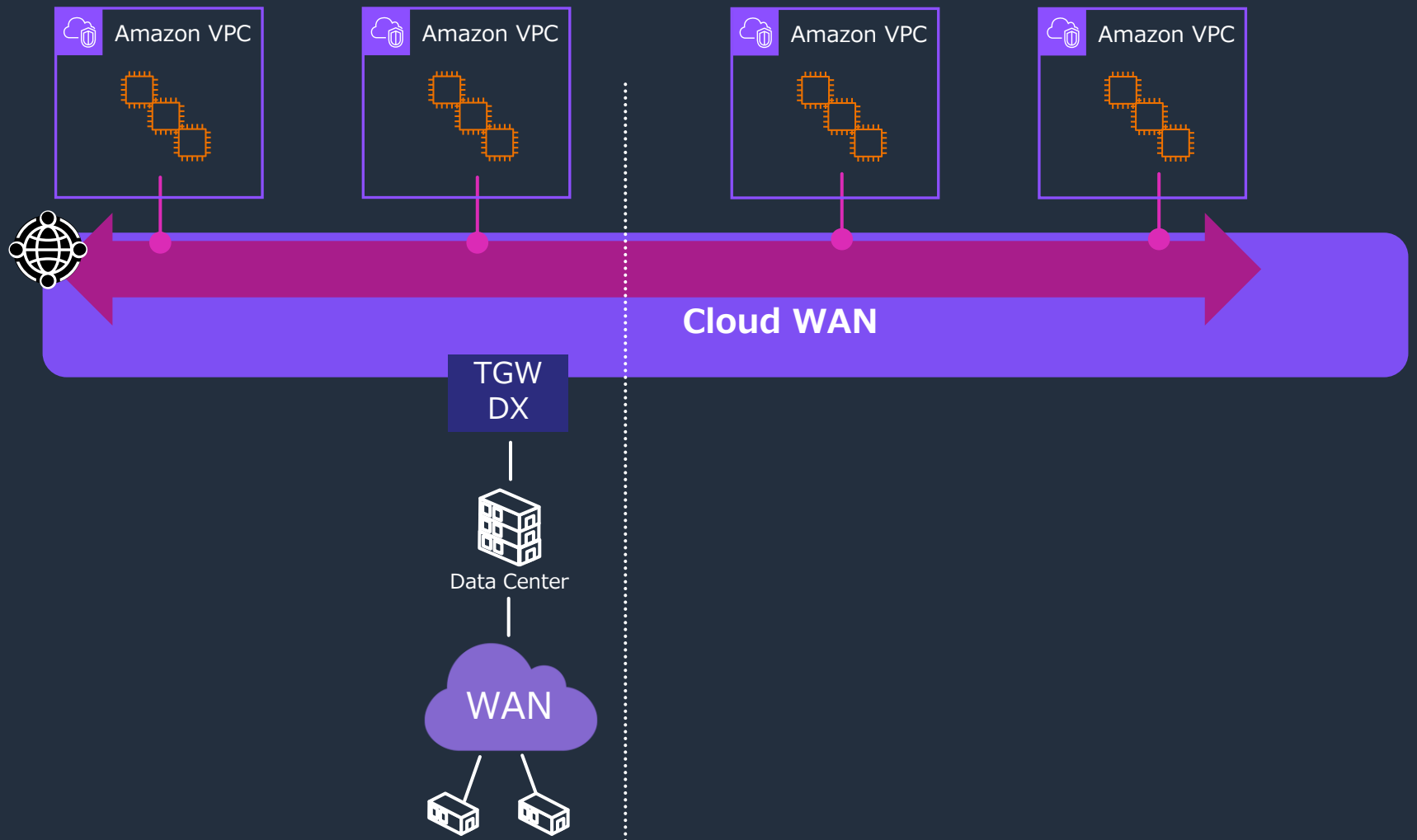
リージョンの追加例（DR対策）



ユースケース

DR対策

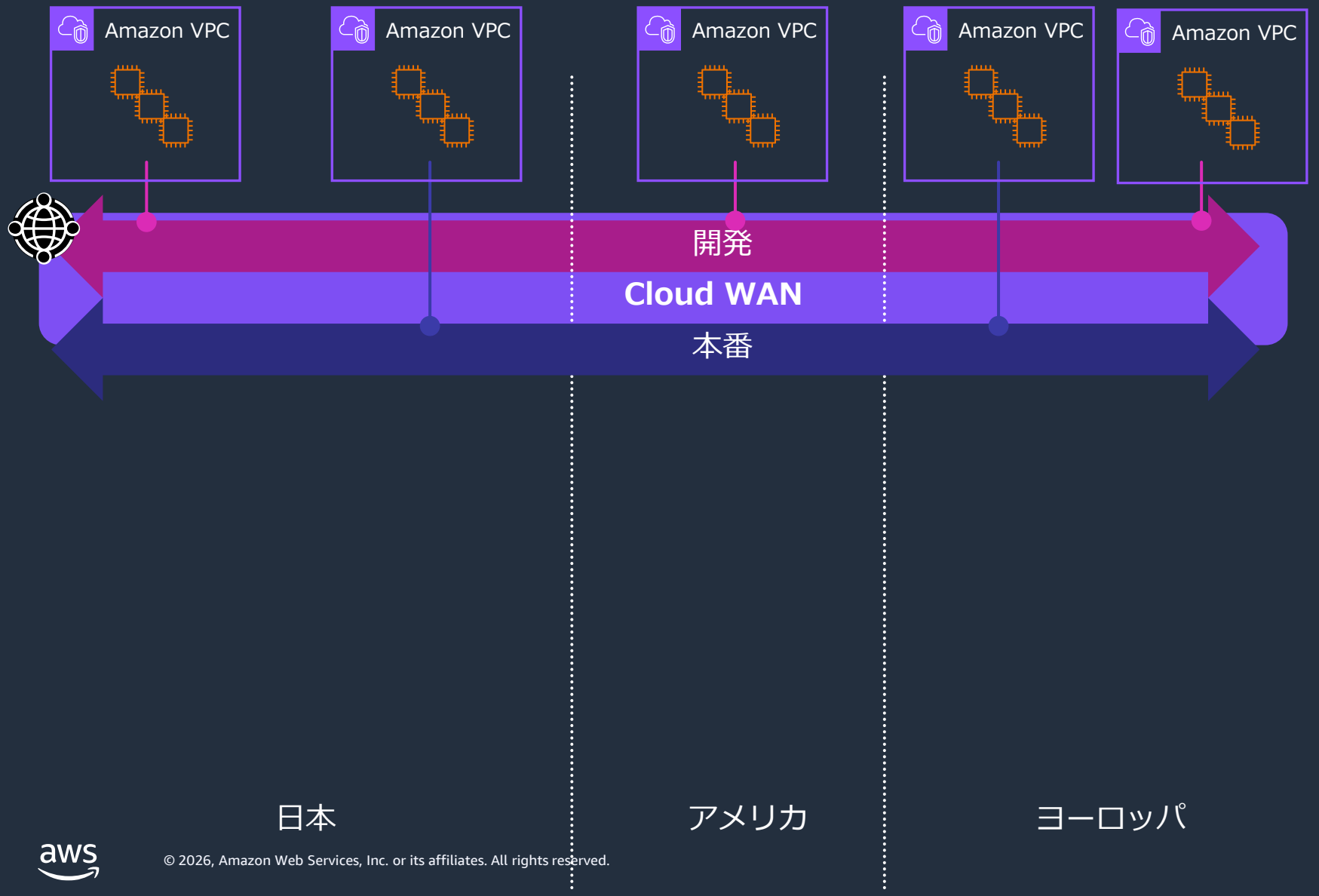
リージョンの追加例（DR対策）



ユースケース

DR対策

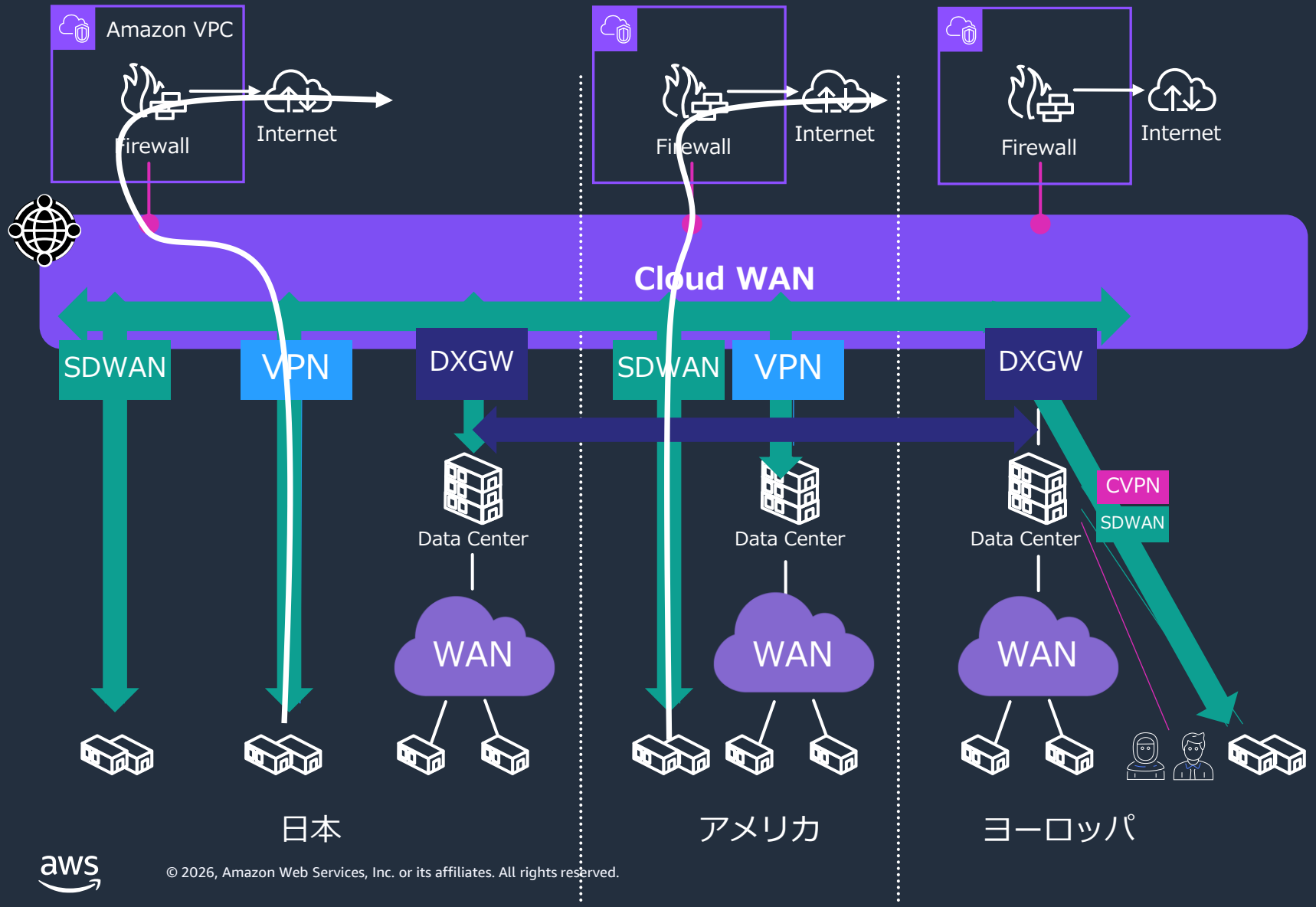
VPC間接続例



ユースケース

VPC間をグローバルなフラットネットワークで接続し、かつネットワークをセグメンテーションしルーティングを分ける。

WAN接続例



ユースケース

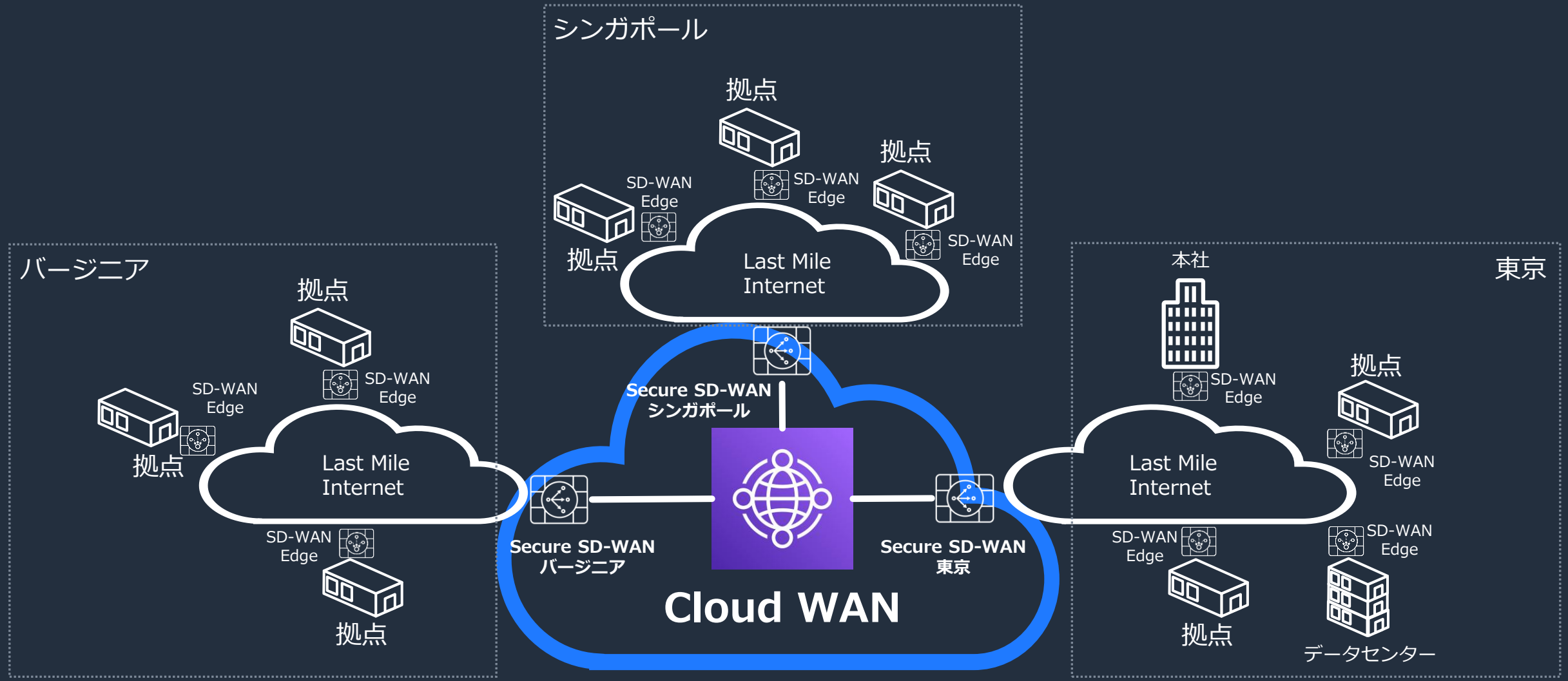
各オンプレミス拠点間をグローバルなフラットネットワークで接続しルーティング行う。SiteLinkとの併用も可能。

インターネットの出口は、AWSの各リージョンごとに個別設定する事も可能。

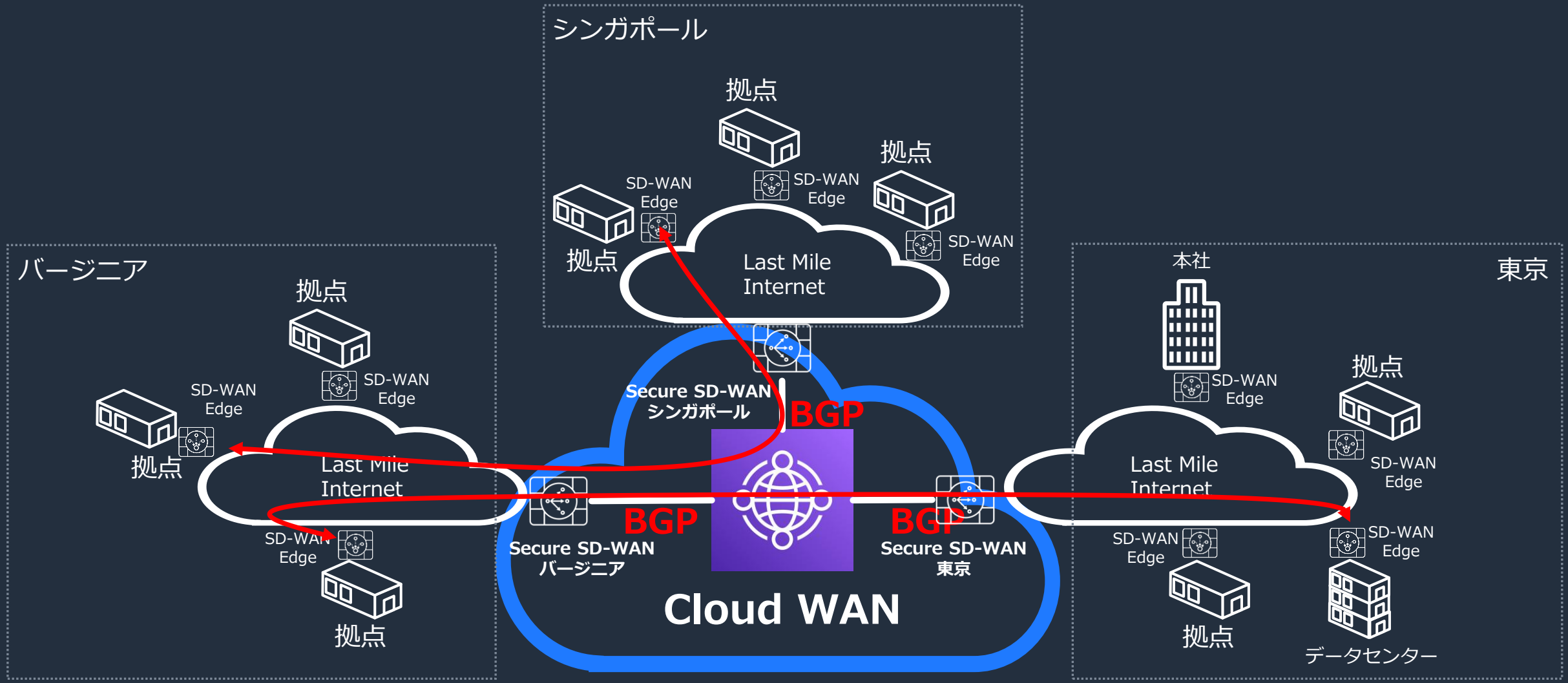
Cloud Native WAN

Cloud WAN SD-WAN連携

Cloud WANをSD-WANのグローバルL3ハブとして活用

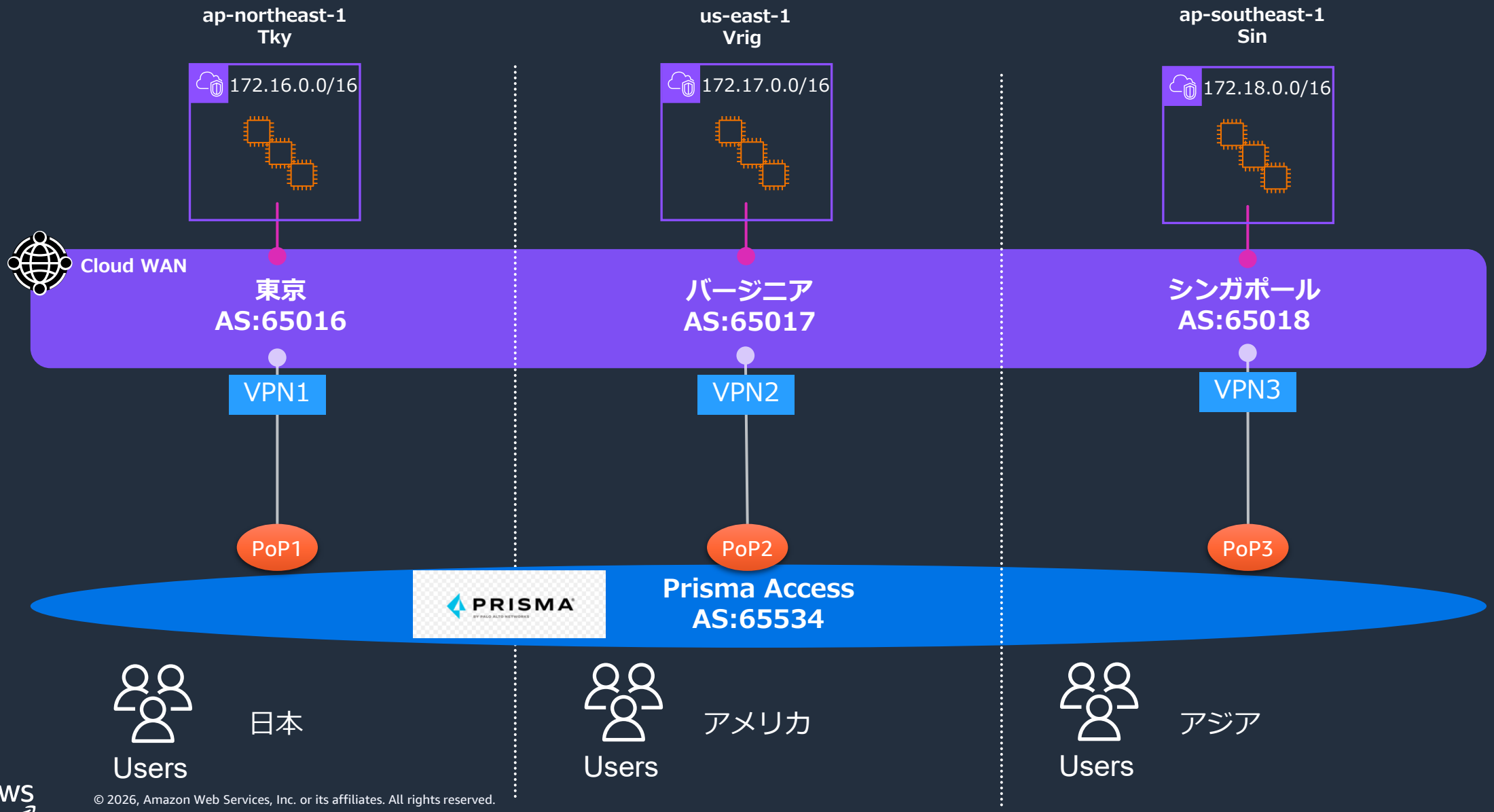


Cloud WANをSD-WANのグローバルL3ハブとして活用

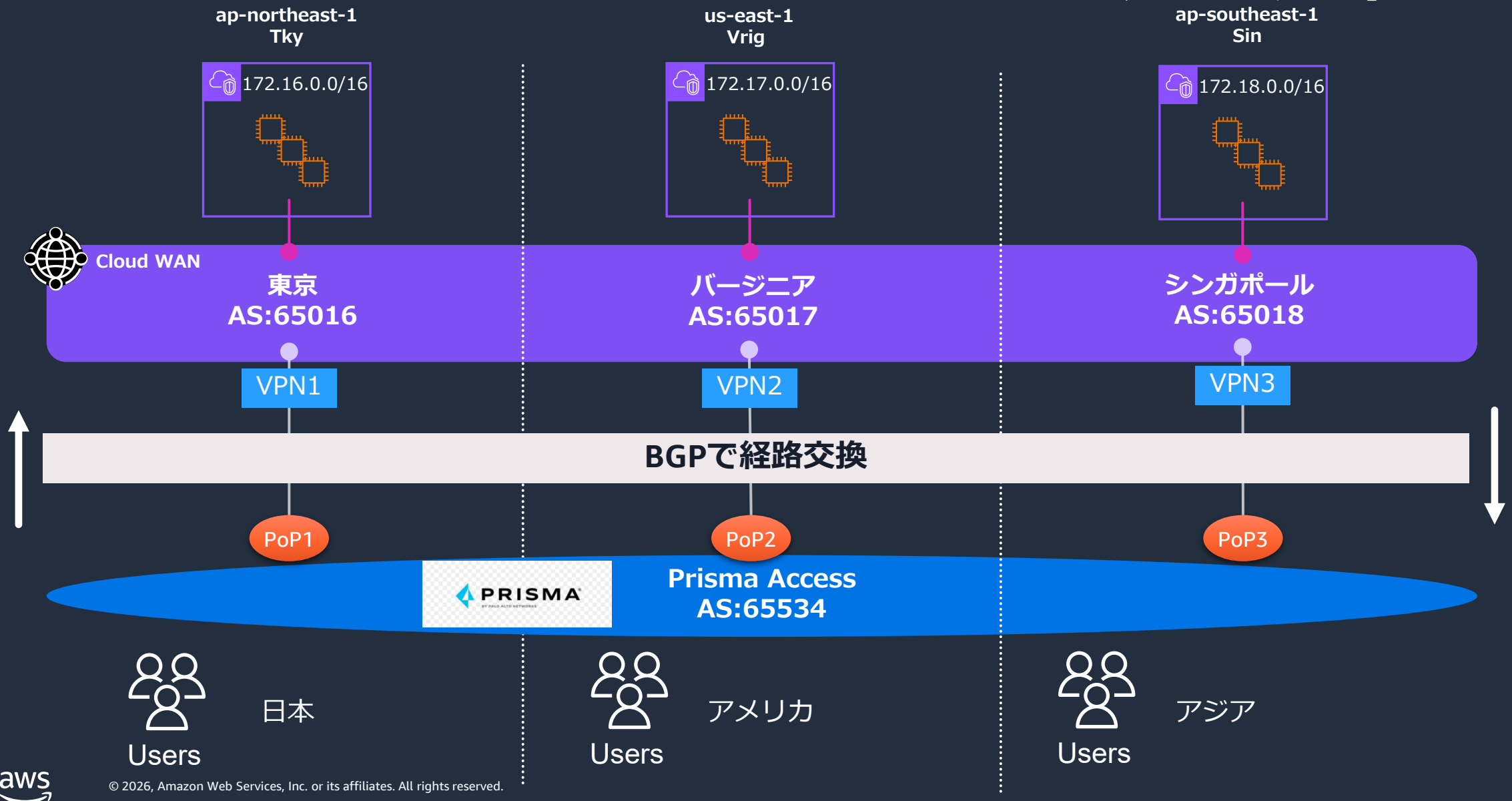


Cloud WAN SASE連携

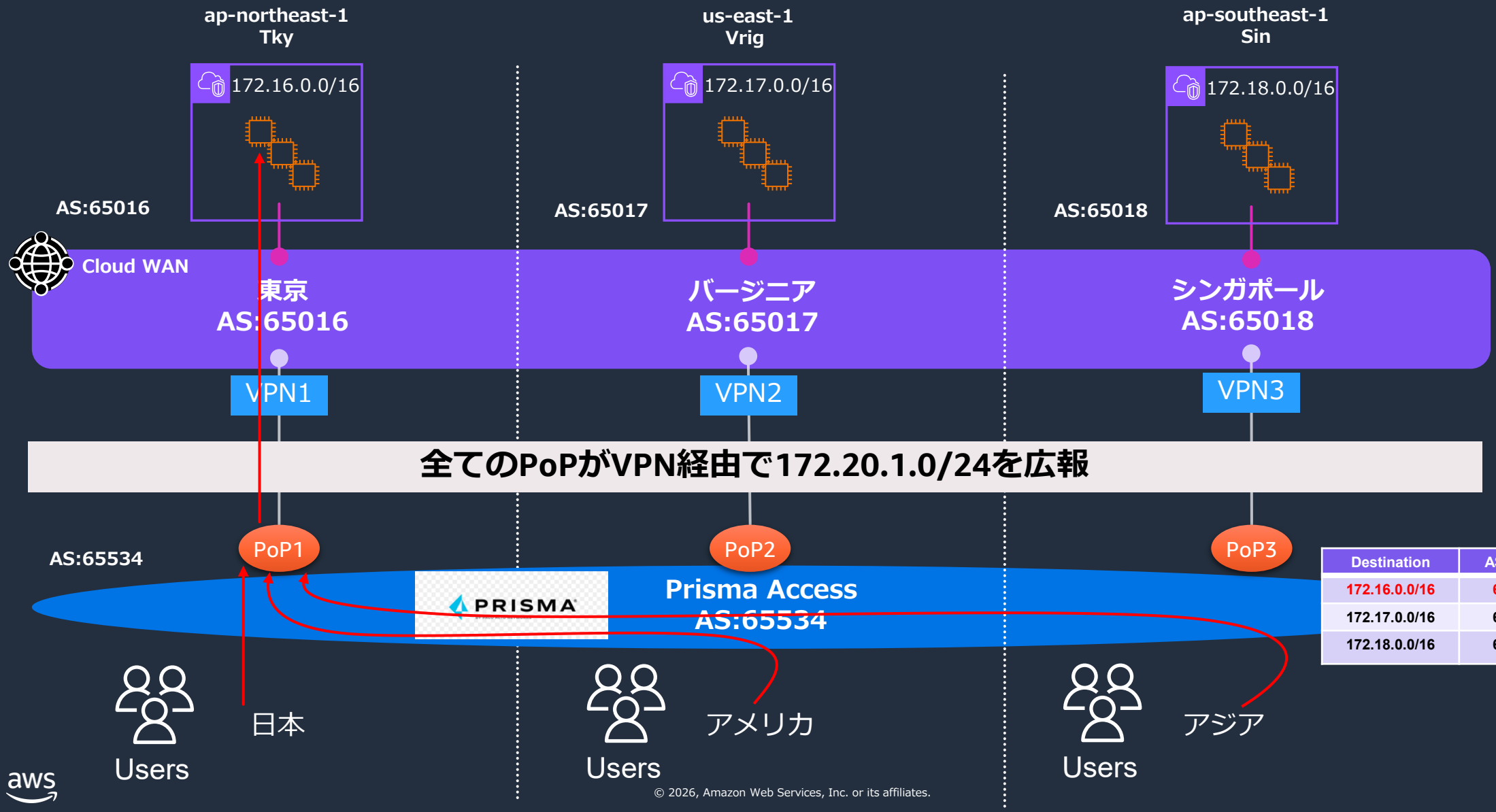
Prisma AccessとCloud WANのルーティング



Prisma AccessとCloud WANのルーティング

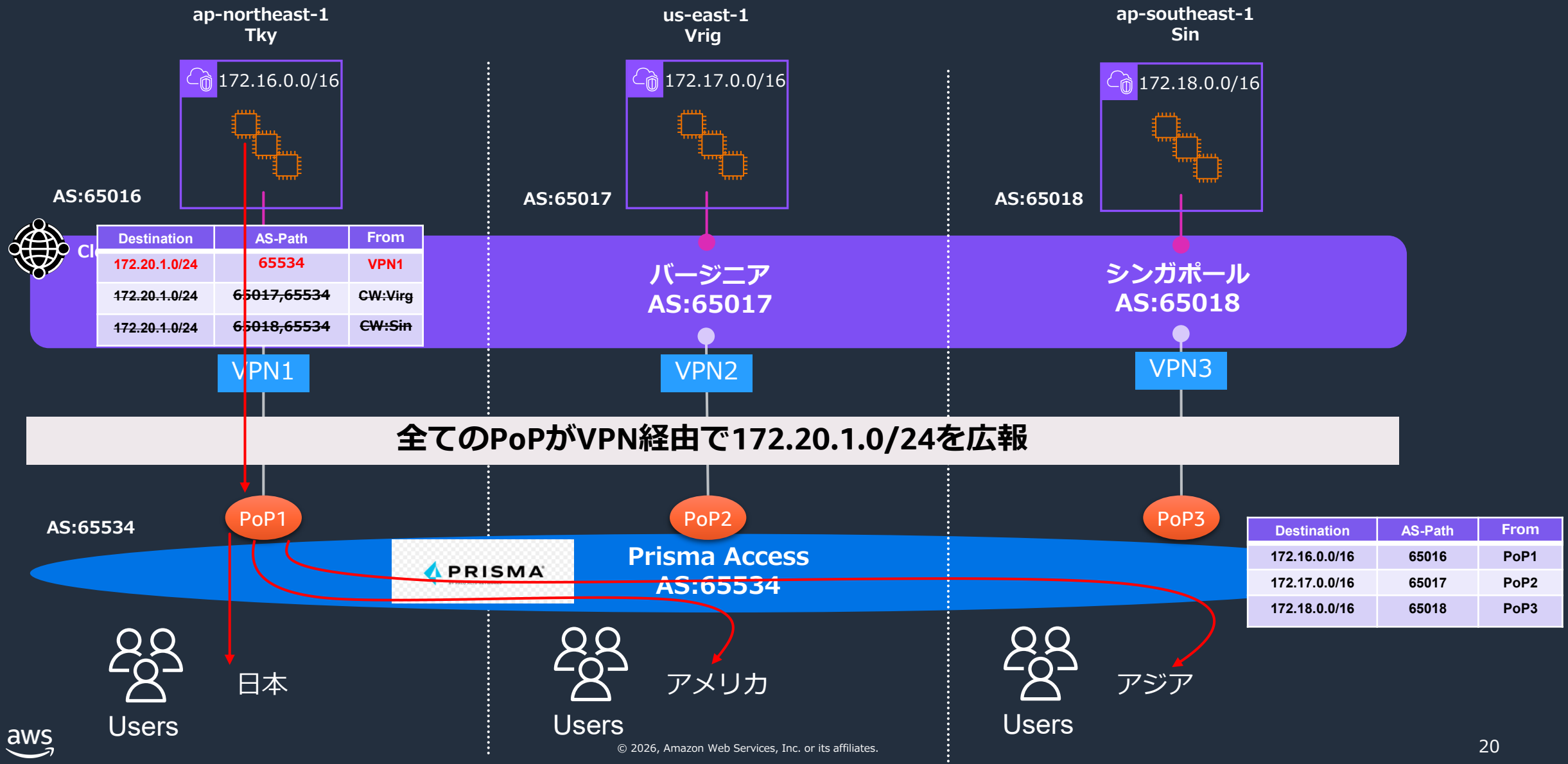


Prisma Access→Cloud WANへのルーティング



Destination	AS-Path	From
172.16.0.0/16	65016	PoP1
172.17.0.0/16	65017	PoP2
172.18.0.0/16	65018	PoP3

Cloud WAN→Prisma Accessへのルーティング



Cloud WANの便利な機能

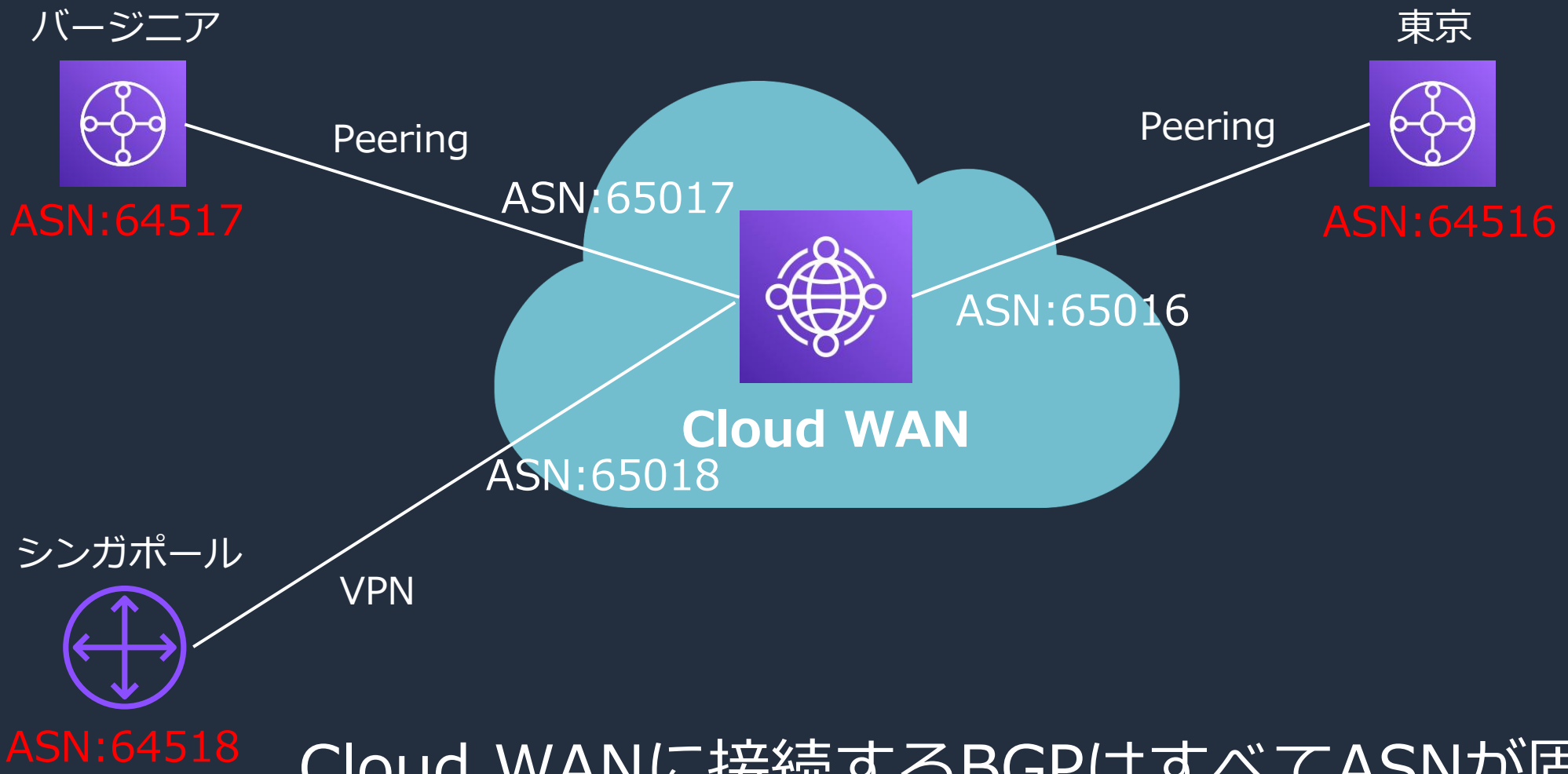
Advanced Routing

Advanced Routing

- BGP経路制御が方法が追加され、より細かなRouting制御が可能

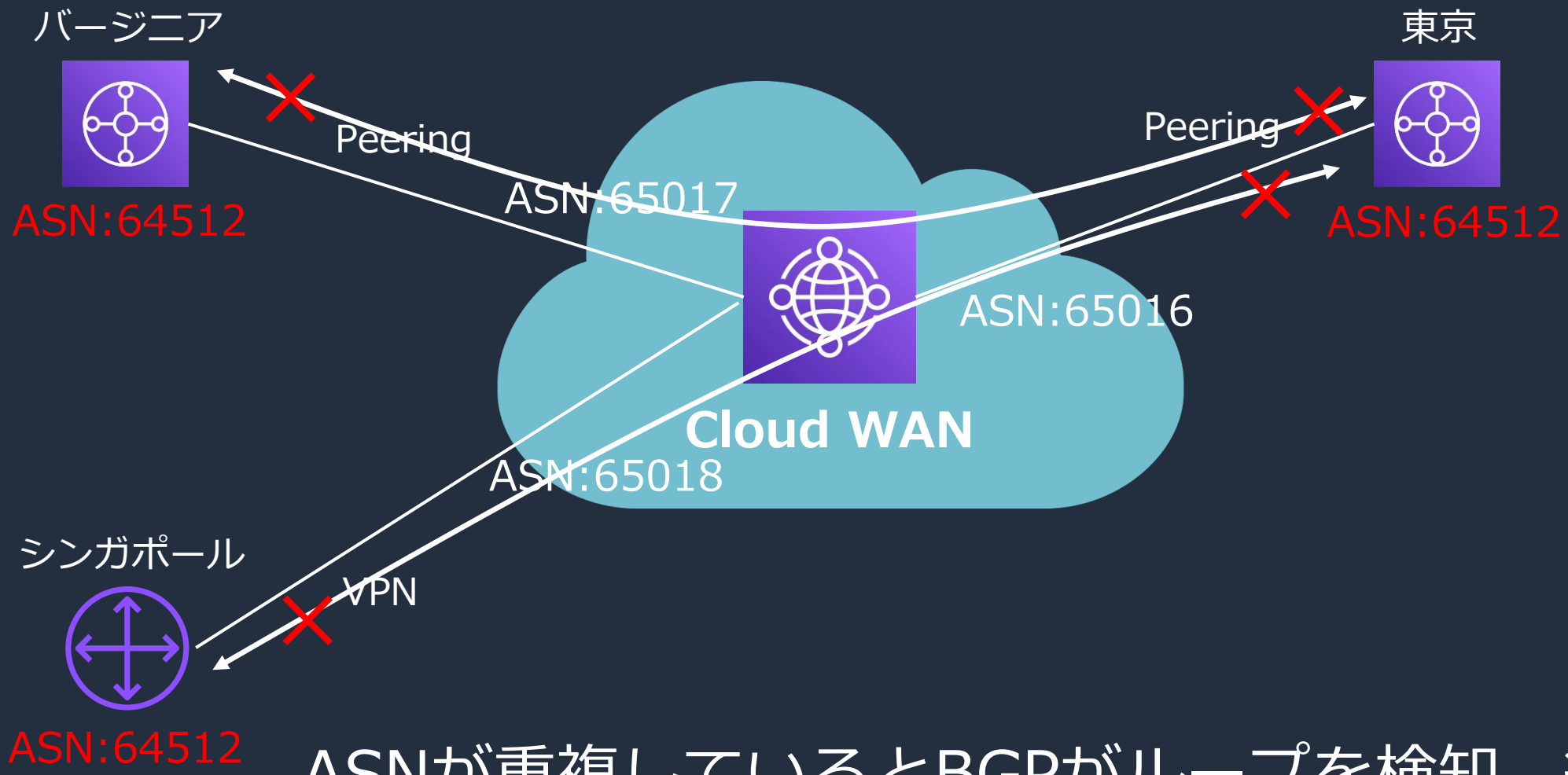
Advanced Routing Policy Rules Match/Action Types		
No	**Match Condition Types**	**Description**
1	prefix-equals	Match IPv4 or IPv6 prefixes
2	prefix-in-cidr	Match prefix that is part of a CIDR space
3	prefix-in-prefix-list	Match prefixes defined in a prefix list
4	asn-in-as-path	Match ASN in as path
5	community-in-list	Match community in the list of BGP communities
6	med-equals	Match MED value
No	**Action Types**	**Description**
1	drop	Drop matched prefixes in the route updates
2	allow	Only allow matched prefixes in the route updates
3	summarize	Summarize routes in route updates
4	prepend-asn-list remove-asn-list replace-asn-list	Add or remove ASNs to the AS-PATH of the route update Replace AS-PATH with a new ASN list
5	add-community remove-community	Add or remove community in the route update
6	set-med	Set MED value in the route update
7	set-local-preference	Set local preference in the route update

Advanced Routing（ Remove ASNサポート前）



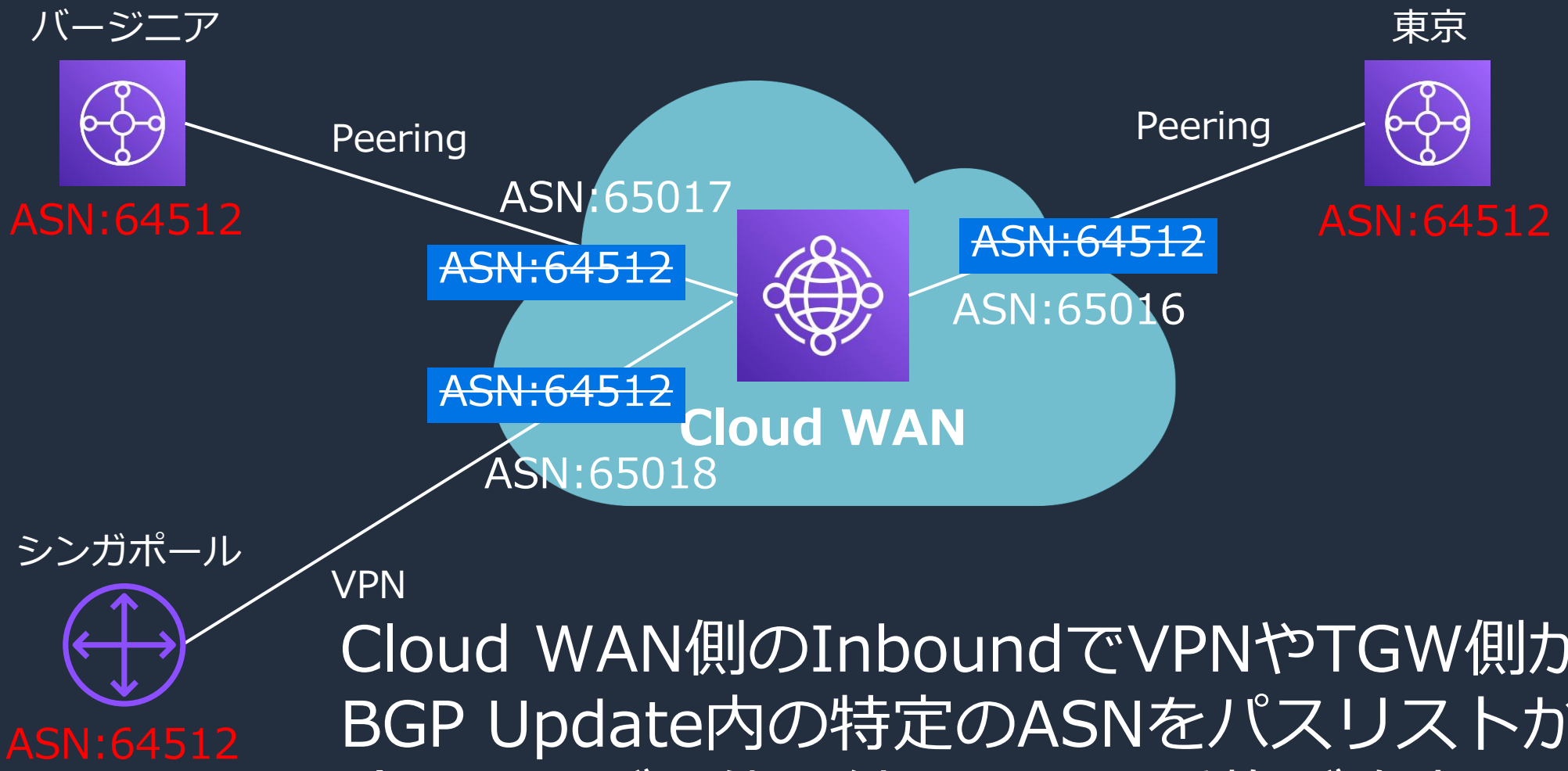
Cloud WANに接続するBGPはすべてASNが固有にする必要があった。

Advanced Routing（ Remove ASNサポート前）



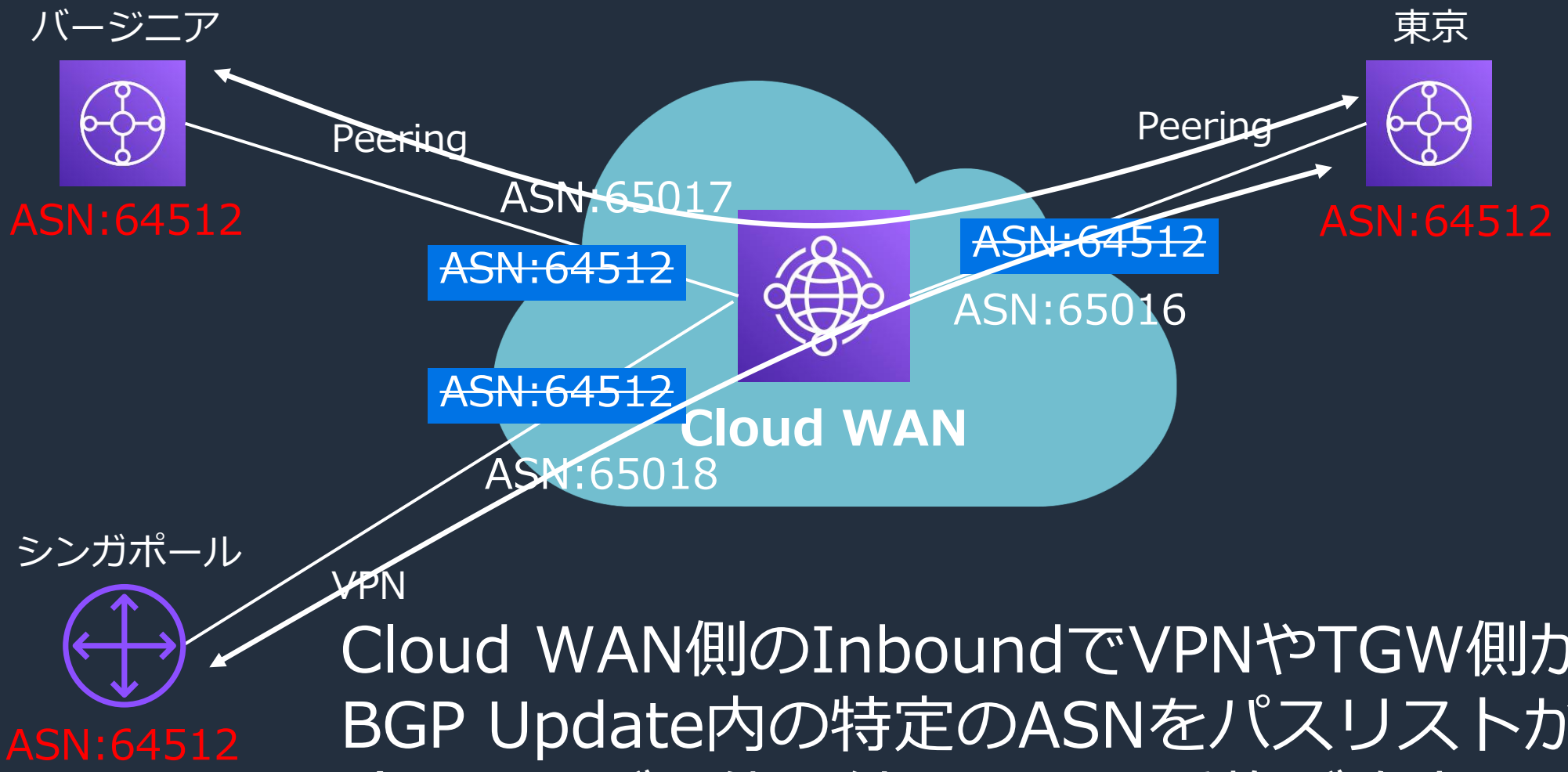
ASNが重複しているとBGPがループを検知。結果Routingができない。

Advanced Routing（Remove ASN）



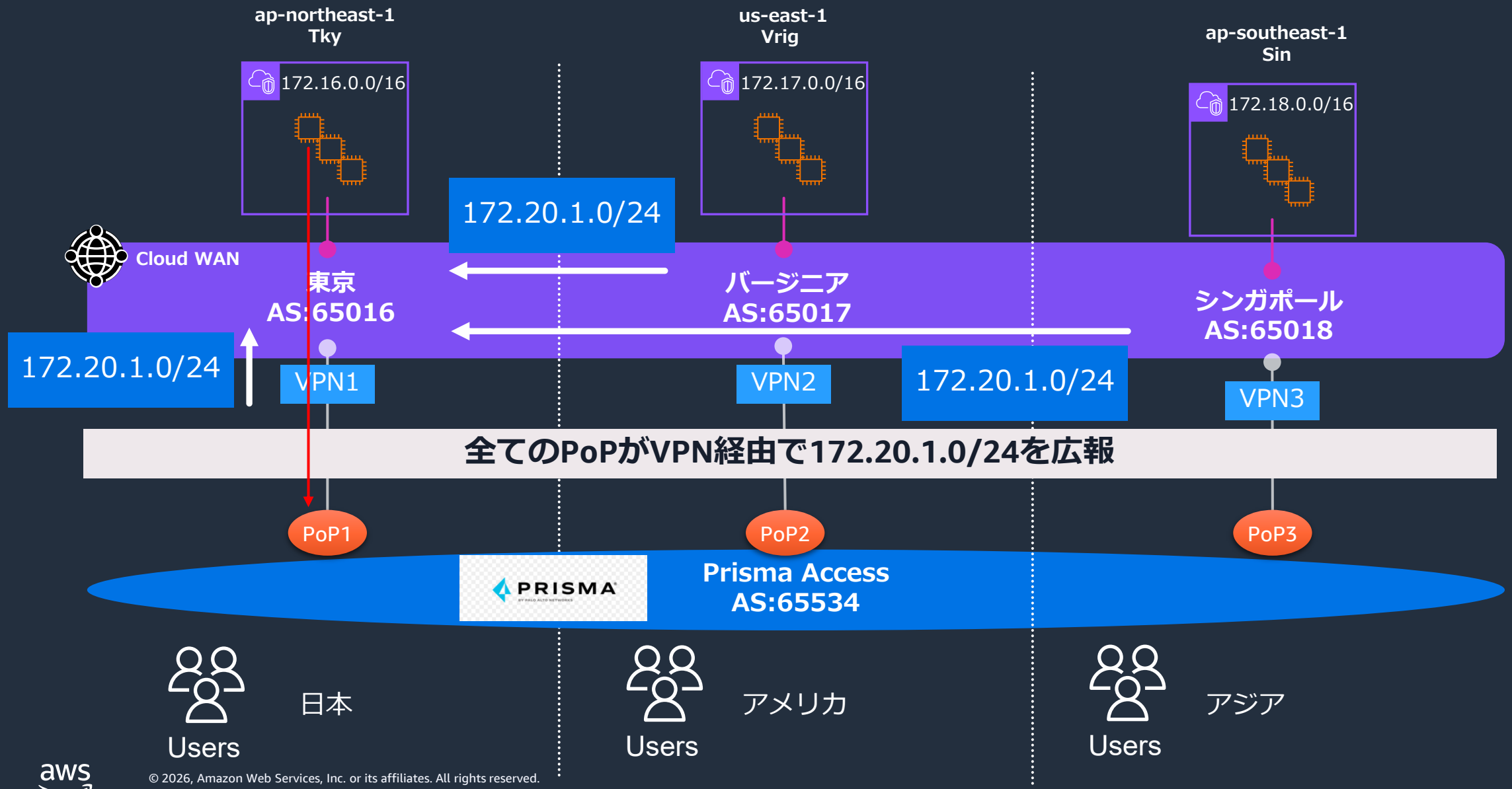
Cloud WAN側のInboundでVPNやTGW側からのBGP Update内の特定のASNをパスリストから取り除くことが可能。結果ASNの重複が許容される。

Advanced Routing（Remove ASN）

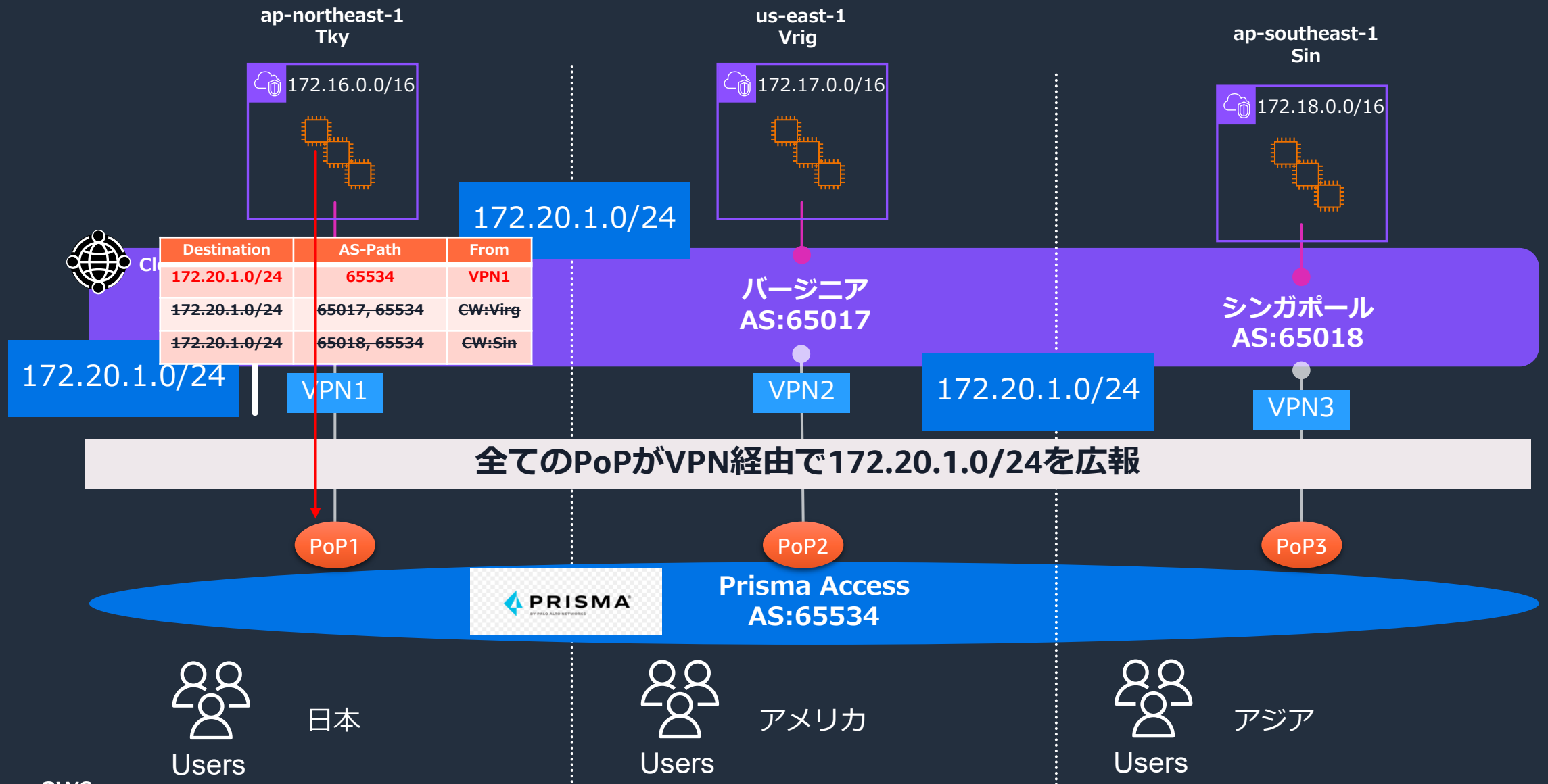


Cloud WAN側のInboundでVPNやTGW側からのBGP Update内の特定のASNをパスリストから取り除くことが可能。結果ASNの重複が許容される。

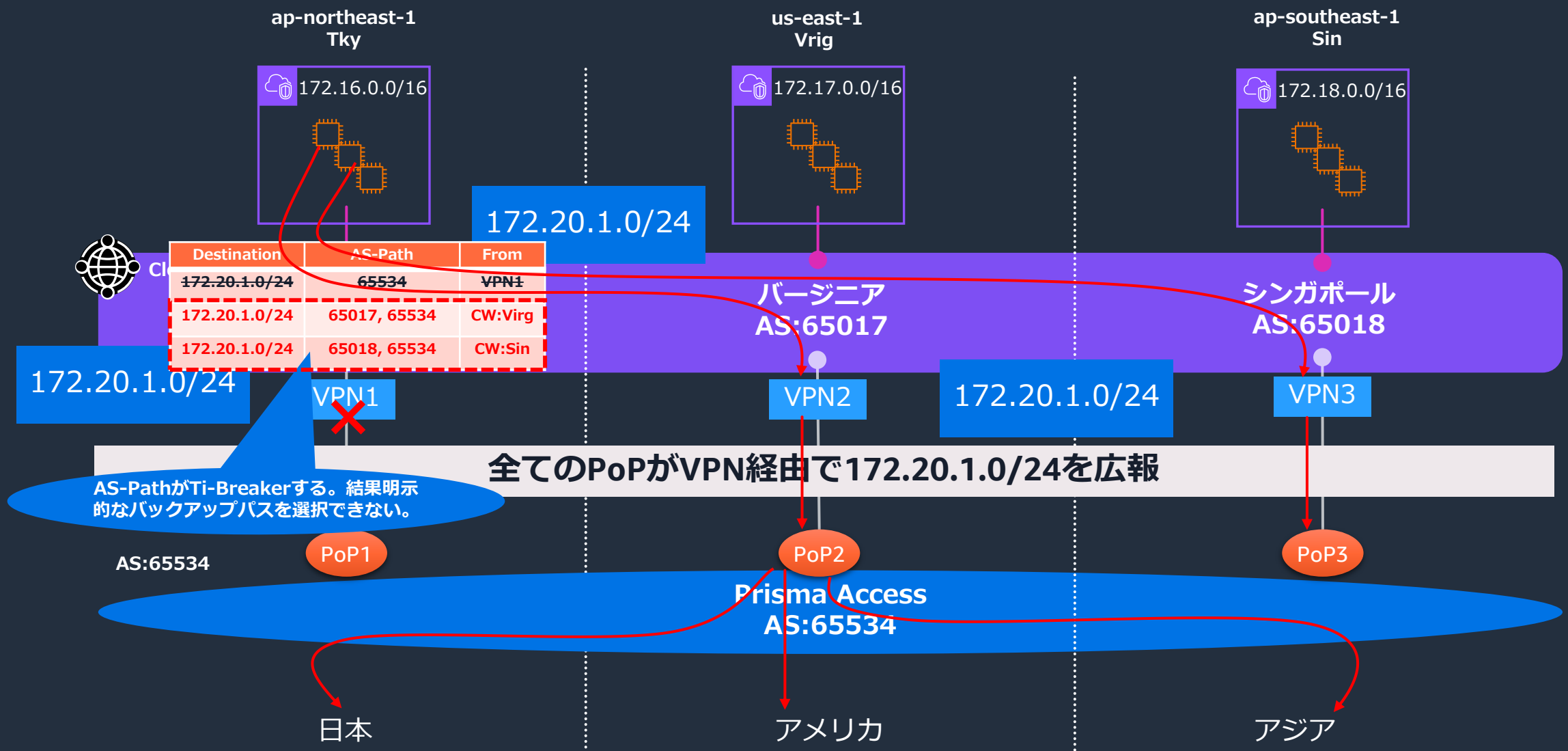
Advanced Routing（**Local Preference無し**）



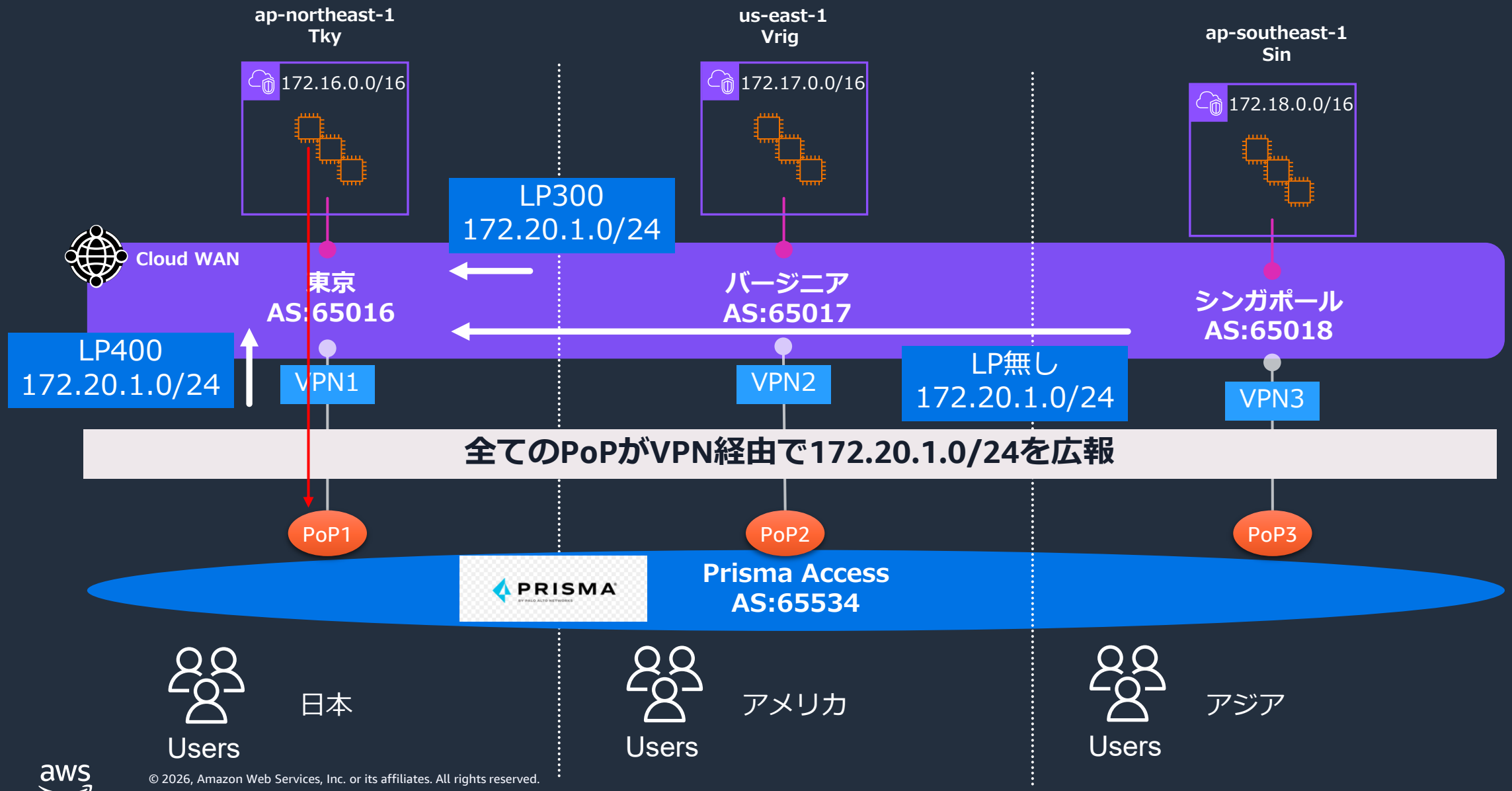
Advanced Routing（**Local Preference無し**）



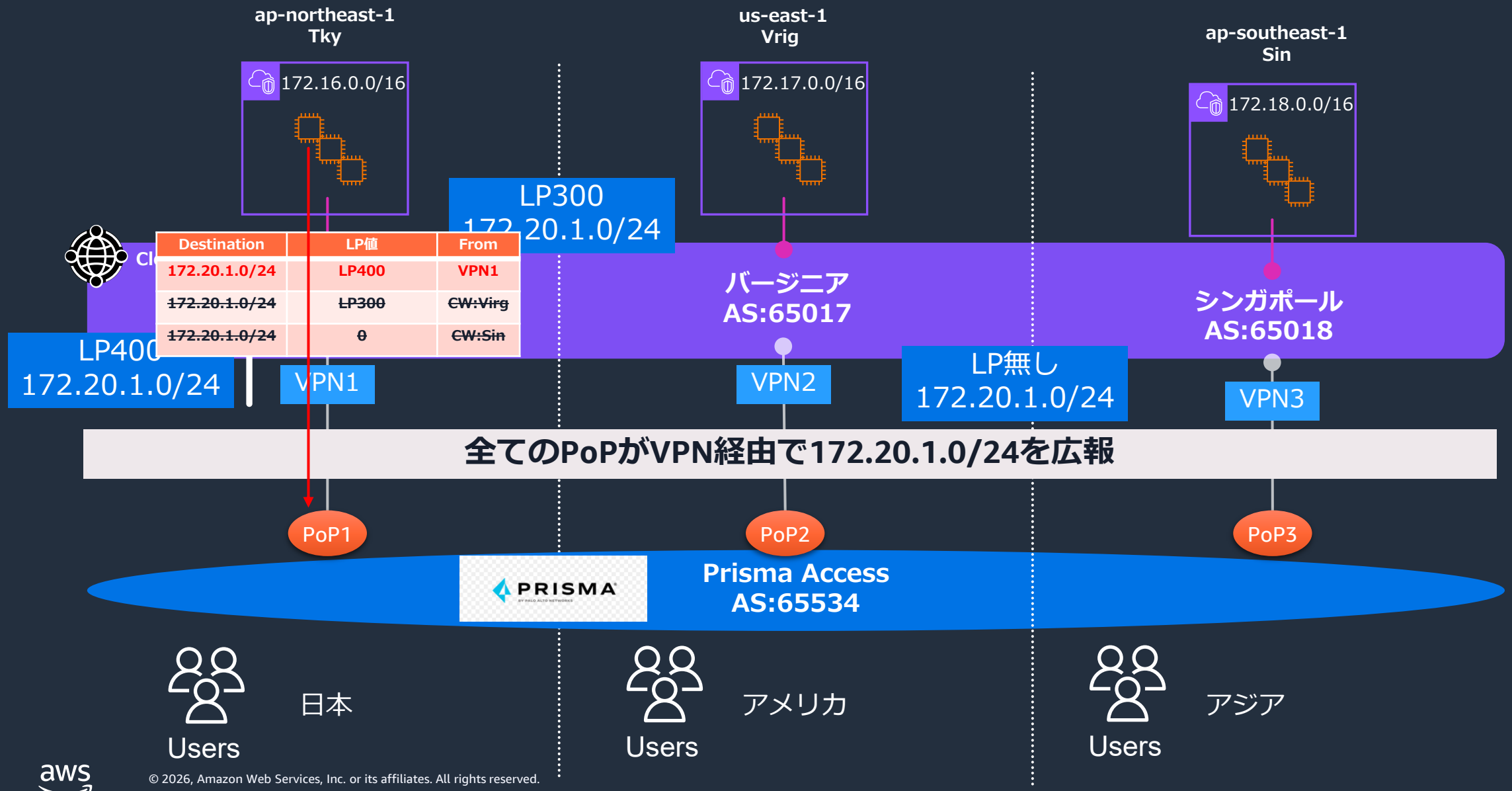
Advanced Routing（Local Preference無し）VPN1障害



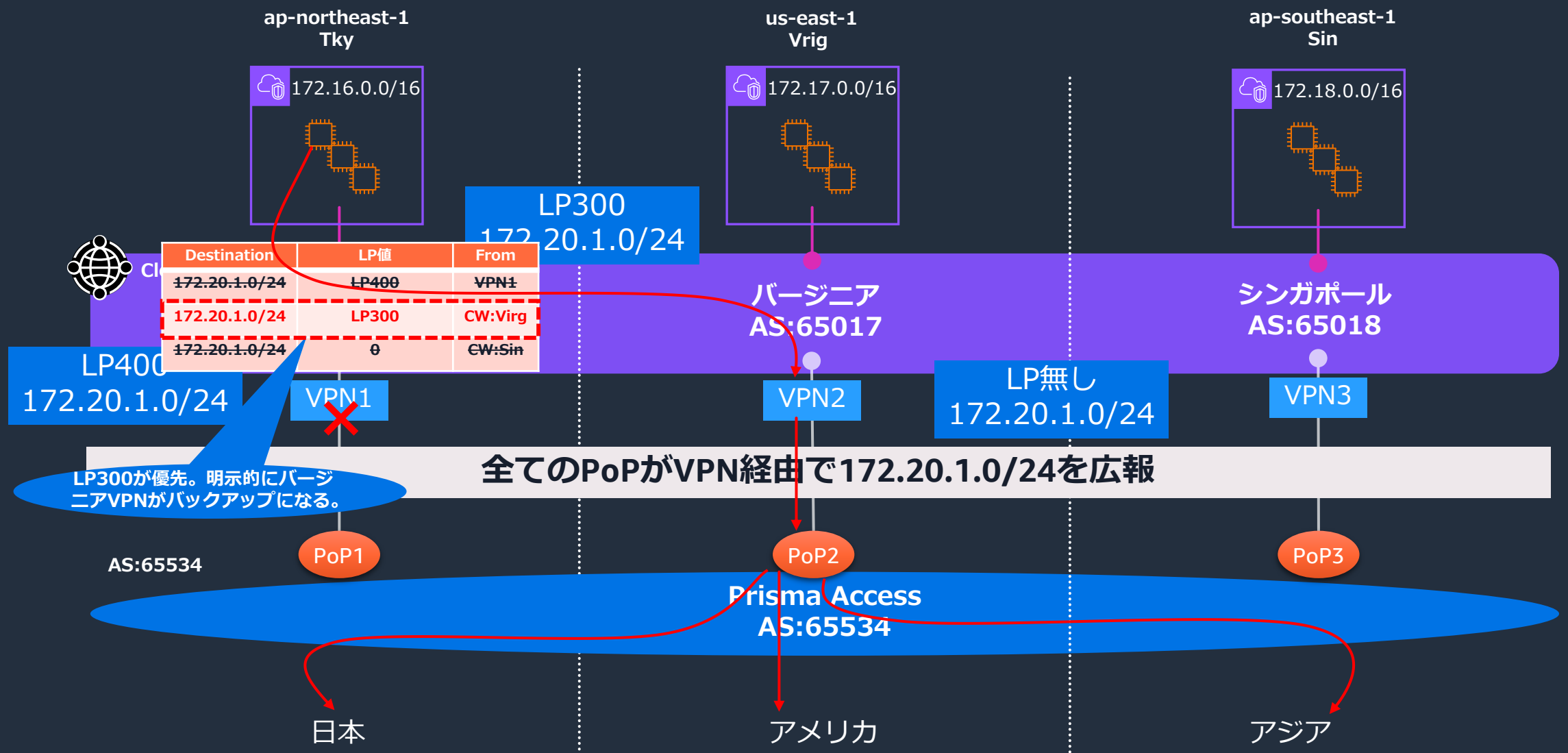
Advanced Routing（**Local Preference**）



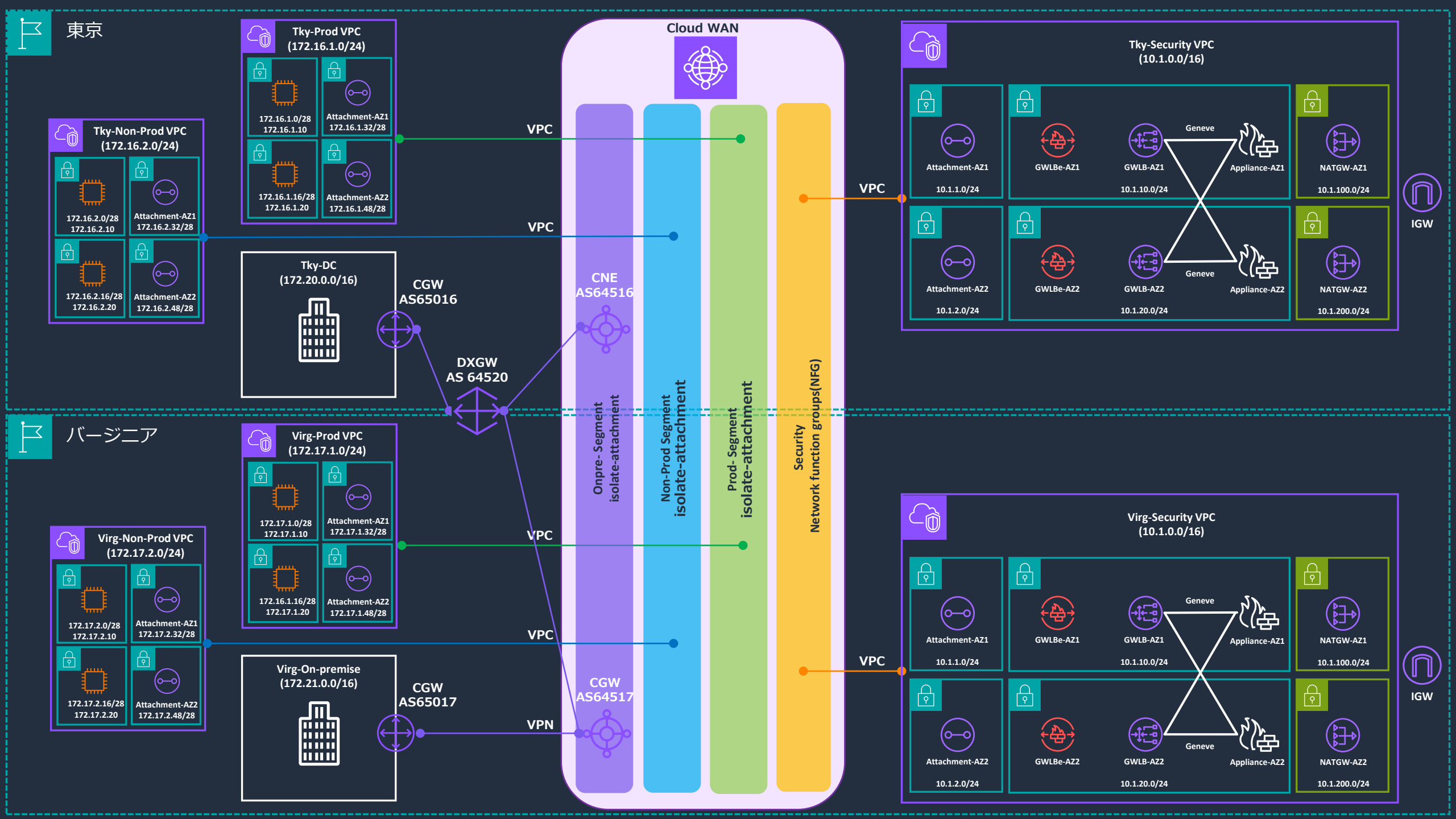
Advanced Routing（**Local Preference**）

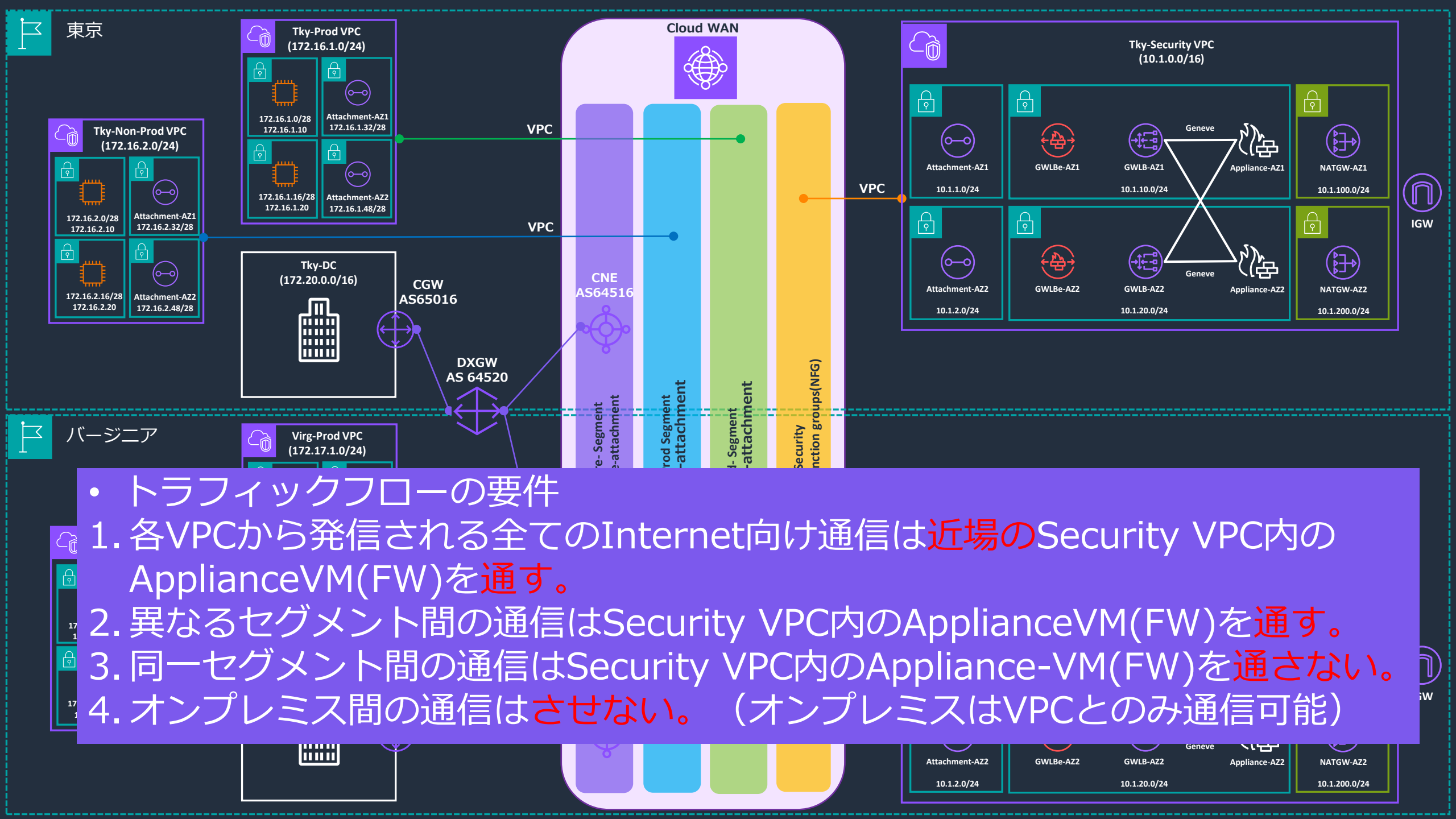


Advanced Routing（Local Preference）VPN1障害



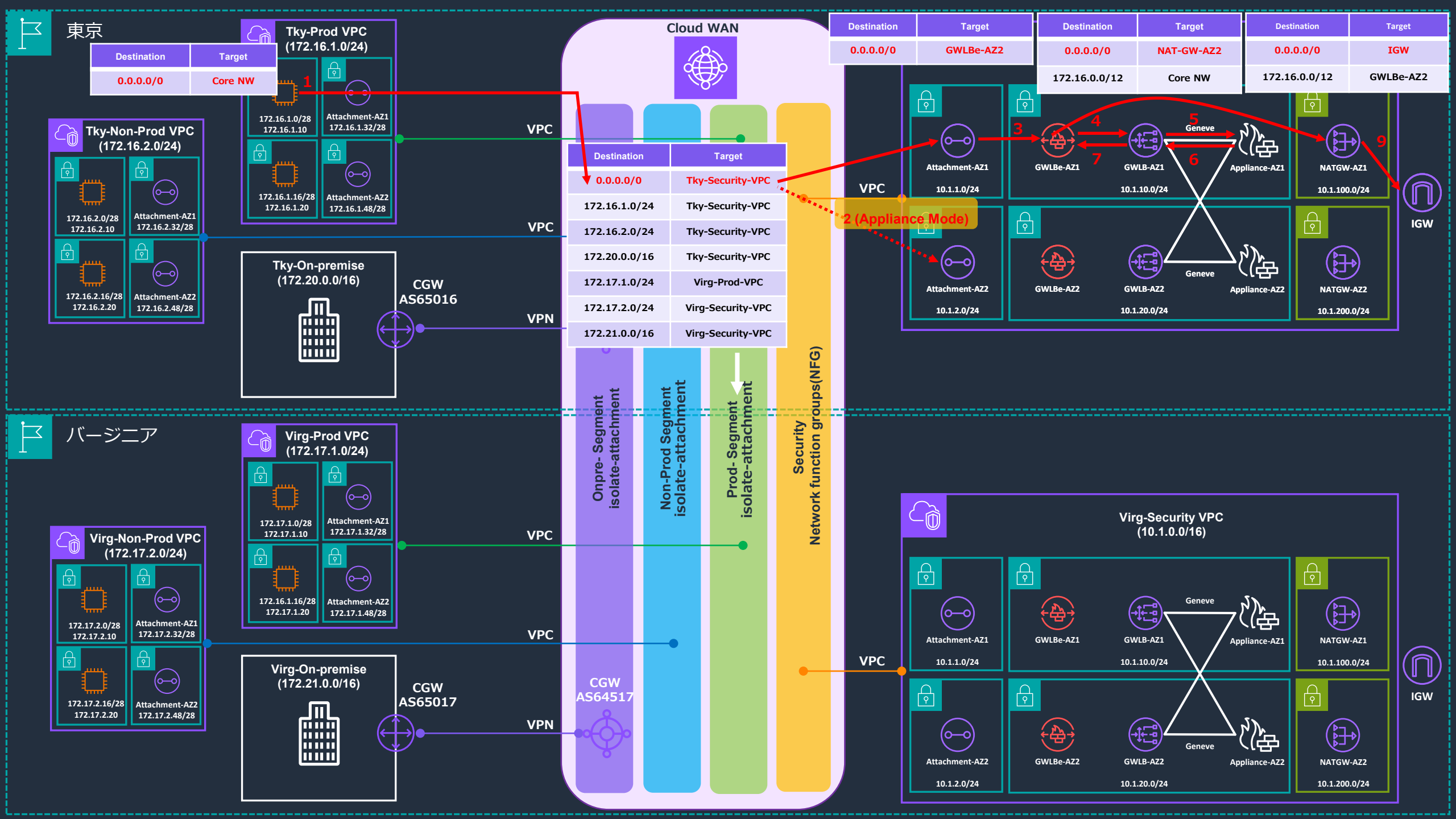
Service Insertion

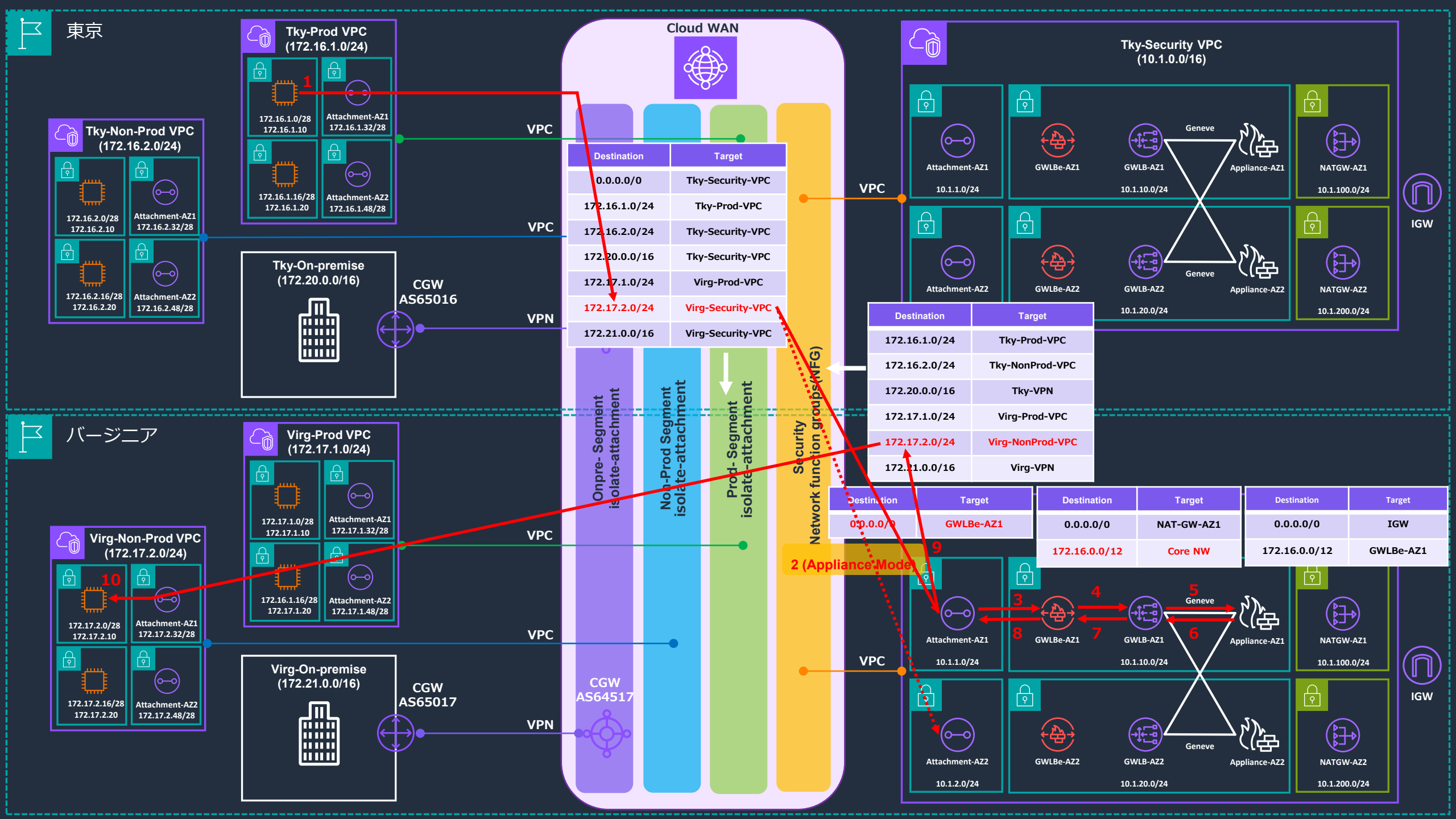

東京
Tky-Prod VPC
(172.16.1.0/24)
172.16.1.0/28
172.16.1.10
Attachment-AZ1
172.16.1.32/28
172.16.1.16/28
172.16.1.20
Attachment-AZ2
172.16.1.48/28
Tky-Non-Prod VPC
(172.16.2.0/24)
172.16.2.0/28
172.16.2.10
Attachment-AZ1
172.16.2.32/28
172.16.2.16/28
172.16.2.20
Attachment-AZ2
172.16.2.48/28
Tky-DC
(172.20.0.0/16)
CGW
AS65016
DXGW
AS 64520
Cloud WAN
CNE
AS64516
Onpre- Segment
isolate-attachment
Non-Prod Segment
isolate-attachment
Prod- Segment
isolate-attachment
Security
Network function groups(NFG)
VPC
VPC
VPC
Tky-Security VPC
(10.1.0.0/16)
Attachment-AZ1
10.1.1.0/24
GWLBe-AZ1
GWLB-AZ1
Geneve
Appliance-AZ1
NATGW-AZ1
10.1.100.0/24
10.1.10.0/24
Attachment-AZ2
10.1.2.0/24
GWLBe-AZ2
GWLB-AZ2
Geneve
Appliance-AZ2
NATGW-AZ2
10.1.200.0/24
10.1.20.0/24
IGW
バージニア
Virg-Prod VPC
(172.17.1.0/24)
172.17.1.0/28
172.17.1.10
Attachment-AZ1
172.17.1.32/28
172.16.1.16/28
172.17.1.20
Attachment-AZ2
172.17.1.48/28
Virg-Non-Prod VPC
(172.17.2.0/24)
172.17.2.0/28
172.17.2.10
Attachment-AZ1
172.17.2.32/28
172.17.2.16/28
172.17.2.20
Attachment-AZ2
172.17.2.48/28
Virg-On-premise
(172.21.0.0/16)
CGW
AS65017
CGW
AS64517
VPC
VPC
VPC
VPN
Virg-Security VPC
(10.1.0.0/16)
Attachment-AZ1
10.1.1.0/24
GWLBe-AZ1
GWLB-AZ1
Geneve
Appliance-AZ1
NATGW-AZ1
10.1.100.0/24
10.1.10.0/24
Attachment-AZ2
10.1.2.0/24
GWLBe-AZ2
GWLB-AZ2
Geneve
Appliance-AZ2
NATGW-AZ2
10.1.200.0/24
10.1.20.0/24
IGW



- トラフィックフローの要件

1. 各VPCから発信される全てのInternet向け通信は近場のSecurity VPC内のApplianceVM(FW)を通す。
2. 異なるセグメント間の通信はSecurity VPC内のApplianceVM(FW)を通す。
3. 同一セグメント間の通信はSecurity VPC内のAppliance-VM(FW)を通さない。
4. オンプレミス間の通信はさせない。（オンプレミスはVPCとのみ通信可能）


東京
Destination
Target
0.0.0.0/0
Core NW
Tky-Prod VPC
(172.16.1.0/24)
1
172.16.1.0/28
172.16.1.10
Attachment-AZ1
172.16.1.32/28
172.16.1.16/28
172.16.1.20
Attachment-AZ2
172.16.1.48/28
Tky-Non-Prod VPC
(172.16.2.0/24)
172.16.2.0/28
172.16.2.10
Attachment-AZ1
172.16.2.32/28
172.16.2.16/28
172.16.2.20
Attachment-AZ2
172.16.2.48/28
Tky-On-premise
(172.20.0.0/16)
CGW
AS65016
VPC
VPC
VPN
Cloud WAN
Destination
Target
0.0.0.0/0
Tky-Security-VPC
172.16.1.0/24
Tky-Security-VPC
172.16.2.0/24
Tky-Security-VPC
172.20.0.0/16
Tky-Security-VPC
172.17.1.0/24
Virg-Prod-VPC
172.17.2.0/24
Virg-Security-VPC
172.21.0.0/16
Virg-Security-VPC
Onpre- Segment
isolate-attachment
Non-Prod Segment
isolate-attachment
Prod- Segment
isolate-attachment
Security
Network function groups(NFG)
CGW
AS64517
Destination
Target
0.0.0.0/0
GWLBe-AZ2
Destination
Target
0.0.0.0/0
NAT-GW-AZ2
172.16.0.0/12
Core NW
Destination
Target
0.0.0.0/0
IGW
172.16.0.0/12
GWLBe-AZ2
VPC
2 (Appliance Mode)
Attachment-AZ1
10.1.1.0/24
3
GWLBe-AZ1
4
GWLB-AZ1
10.1.10.0/24
5
Geneve
6
7
Appliance-AZ1
NATGW-AZ1
10.1.100.0/24
9
IGW
Attachment-AZ2
10.1.2.0/24
GWLBe-AZ2
GWLB-AZ2
10.1.20.0/24
Geneve
Appliance-AZ2
NATGW-AZ2
10.1.200.0/24
バージニア
Virg-Prod VPC
(172.17.1.0/24)
172.17.1.0/28
172.17.1.10
Attachment-AZ1
172.17.1.32/28
172.17.1.16/28
172.17.1.20
Attachment-AZ2
172.17.1.48/28
Virg-Non-Prod VPC
(172.17.2.0/24)
172.17.2.0/28
172.17.2.10
Attachment-AZ1
172.17.2.32/28
172.17.2.16/28
172.17.2.20
Attachment-AZ2
172.17.2.48/28
Virg-On-premise
(172.21.0.0/16)
CGW
AS65017
VPC
VPC
VPN
Virg-Security VPC
(10.1.0.0/16)
Attachment-AZ1
10.1.1.0/24
GWLBe-AZ1
GWLB-AZ1
10.1.10.0/24
Geneve
Appliance-AZ1
NATGW-AZ1
10.1.100.0/24
IGW
Attachment-AZ2
10.1.2.0/24
GWLBe-AZ2
GWLB-AZ2
10.1.20.0/24
Geneve
Appliance-AZ2
NATGW-AZ2
10.1.200.0/24

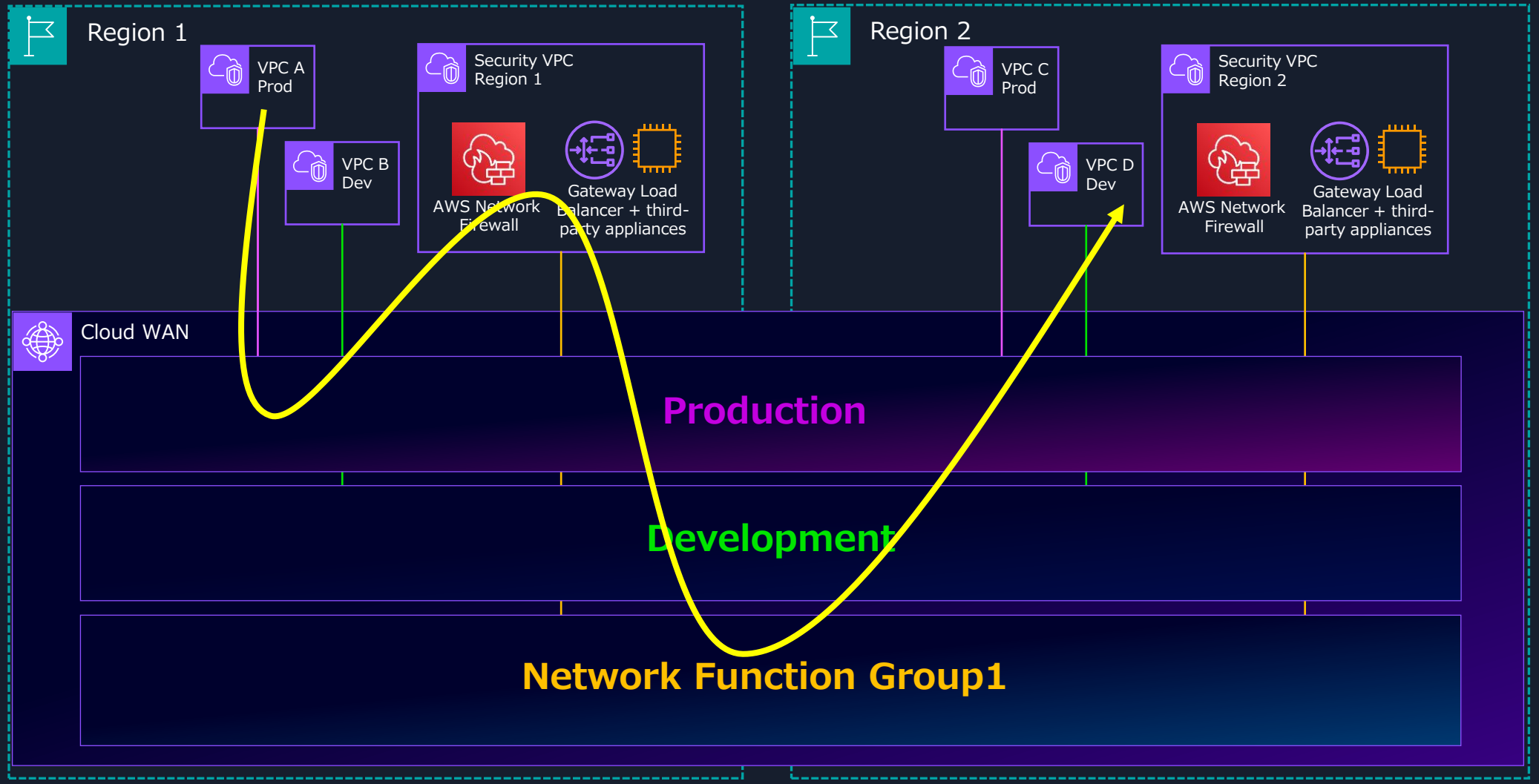

東京
Tky-Prod VPC
(172.16.1.0/24)
172.16.1.0/28
172.16.1.10
Attachment-AZ1
172.16.1.32/28
172.16.1.16/28
172.16.1.20
Attachment-AZ2
172.16.1.48/28
Tky-Non-Prod VPC
(172.16.2.0/24)
172.16.2.0/28
172.16.2.10
Attachment-AZ1
172.16.2.32/28
172.16.2.16/28
172.16.2.20
Attachment-AZ2
172.16.2.48/28
Tky-On-premise
(172.20.0.0/16)
CGW
AS65016
VPC
VPC
VPN
Cloud WAN
Destination
Target
0.0.0.0/0
Tky-Security-VPC
172.16.1.0/24
Tky-Prod-VPC
172.16.2.0/24
Tky-Security-VPC
172.20.0.0/16
Tky-Security-VPC
172.17.1.0/24
Virg-Prod-VPC
172.17.2.0/24
Virg-Security-VPC
172.21.0.0/16
Virg-Security-VPC
Onpre- Segment
isolate-attachment
Non-Prod Segment
isolate-attachment
Prod- Segment
isolate-attachment
Security
Network function groups(NFG)
CGW
AS64517
VPC
Tky-Security VPC
(10.1.0.0/16)
Attachment-AZ1
10.1.1.0/24
GWLBe-AZ1
GWLB-AZ1
10.1.10.0/24
Geneve
Appliance-AZ1
NATGW-AZ1
10.1.100.0/24
Attachment-AZ2
GWLBe-AZ2
GWLB-AZ2
10.1.20.0/24
Appliance-AZ2
NATGW-AZ2
10.1.200.0/24
IGW
Destination
Target
172.16.1.0/24
Tky-Prod-VPC
172.16.2.0/24
Tky-NonProd-VPC
172.20.0.0/16
Tky-VPN
172.17.1.0/24
Virg-Prod-VPC
172.17.2.0/24
Virg-NonProd-VPC
172.21.0.0/16
Virg-VPN
Destination
Target
0.0.0.0/0
GWLBe-AZ1
Destination
Target
0.0.0.0/0
NAT-GW-AZ1
172.16.0.0/12
Core NW
Destination
Target
0.0.0.0/0
IGW
172.16.0.0/12
GWLBe-AZ1
2 (Appliance Mode)
バージニア
Virg-Prod VPC
(172.17.1.0/24)
172.17.1.0/28
172.17.1.10
Attachment-AZ1
172.17.1.32/28
172.16.1.16/28
172.17.1.20
Attachment-AZ2
172.17.1.48/28
Virg-Non-Prod VPC
(172.17.2.0/24)
172.17.2.0/28
172.17.2.10
Attachment-AZ1
172.17.2.32/28
172.17.2.16/28
172.17.2.20
Attachment-AZ2
172.17.2.48/28
Virg-On-premise
(172.21.0.0/16)
CGW
AS65017
VPC
VPC
VPN
1
2 (Appliance Mode)
3
4
5
6
7
8
9
10

これどうやって実現してるの？

- もしかして、グローバルネットワーク全体でCloud WAN内でチクチクStatic Routeを細かく書いてるの？？
- VPCやオンプレミス拠点増えたときどうするの？？（経路が増えたとき）

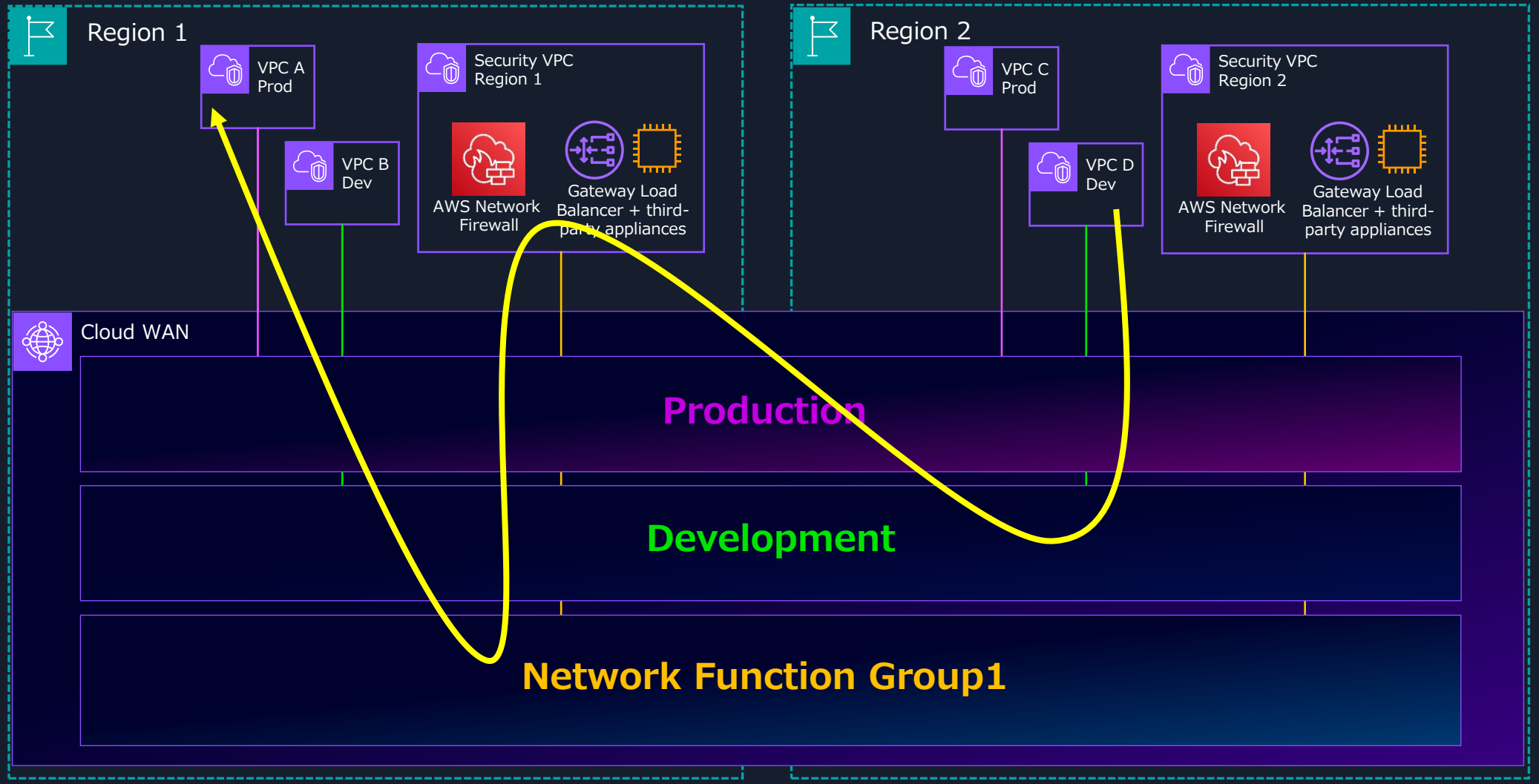
→こんなの手動で行っていたら絶対、設計も設定も破綻します・・・・

Service Insertion機能概要



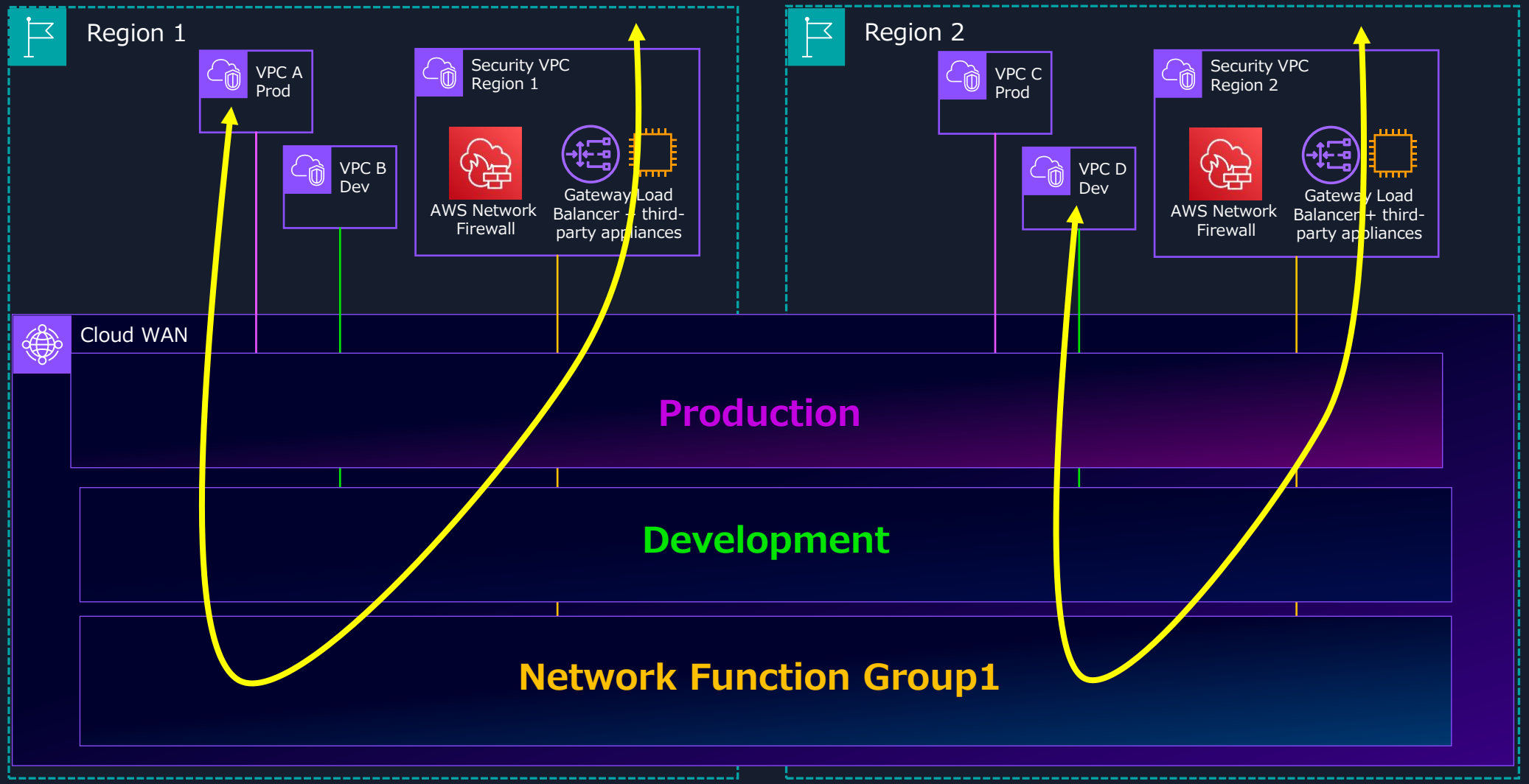
リージョン間のトラフィックインスペクションを制御する機能。

Service Insertion機能概要



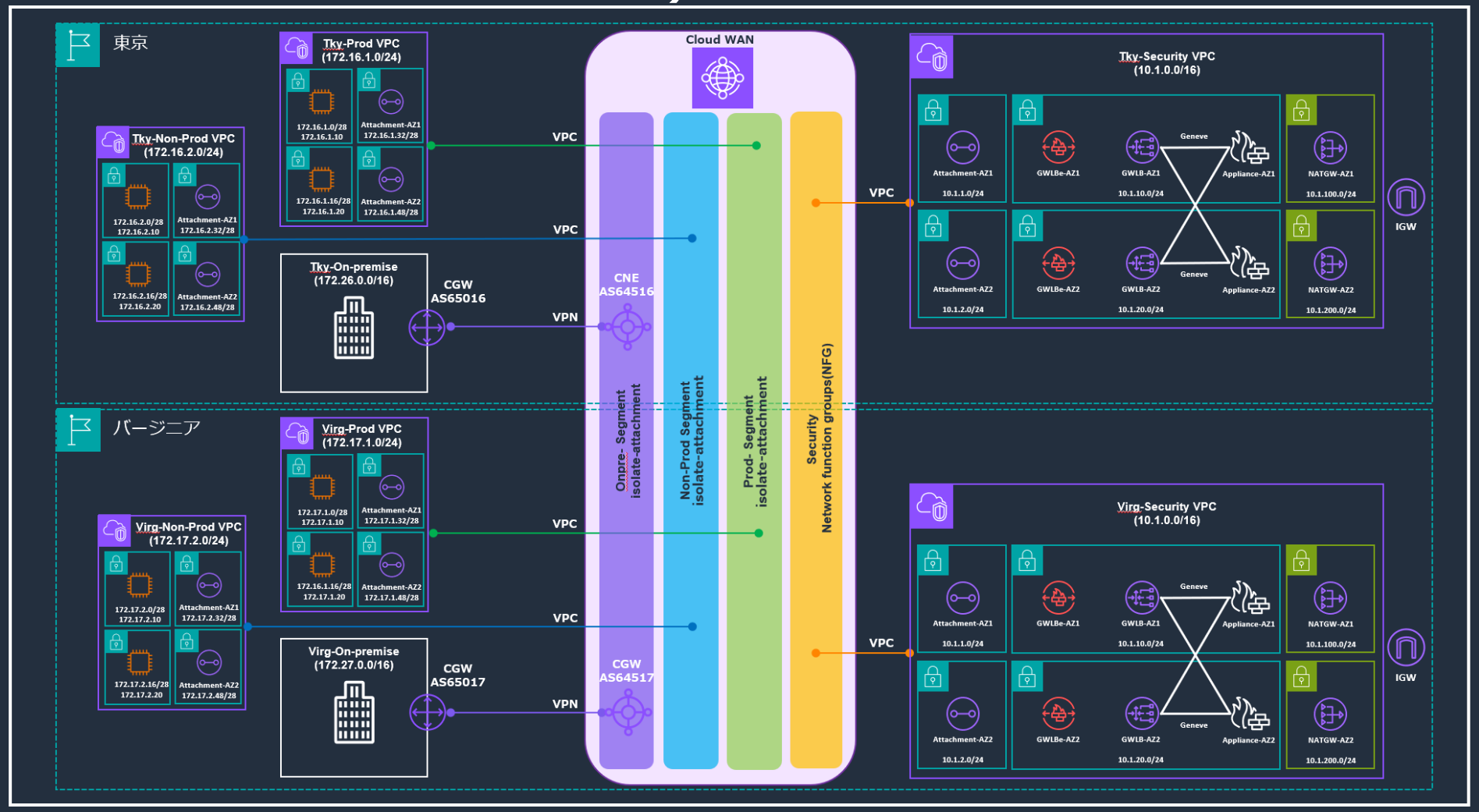
リージョン間のトラフィックインスペクションを制御する機能。

Service Insertion機能概要



「send to」はセグメント内のデフォルトルートを自動生成するモード。

IaC(Infrastructure as Code)



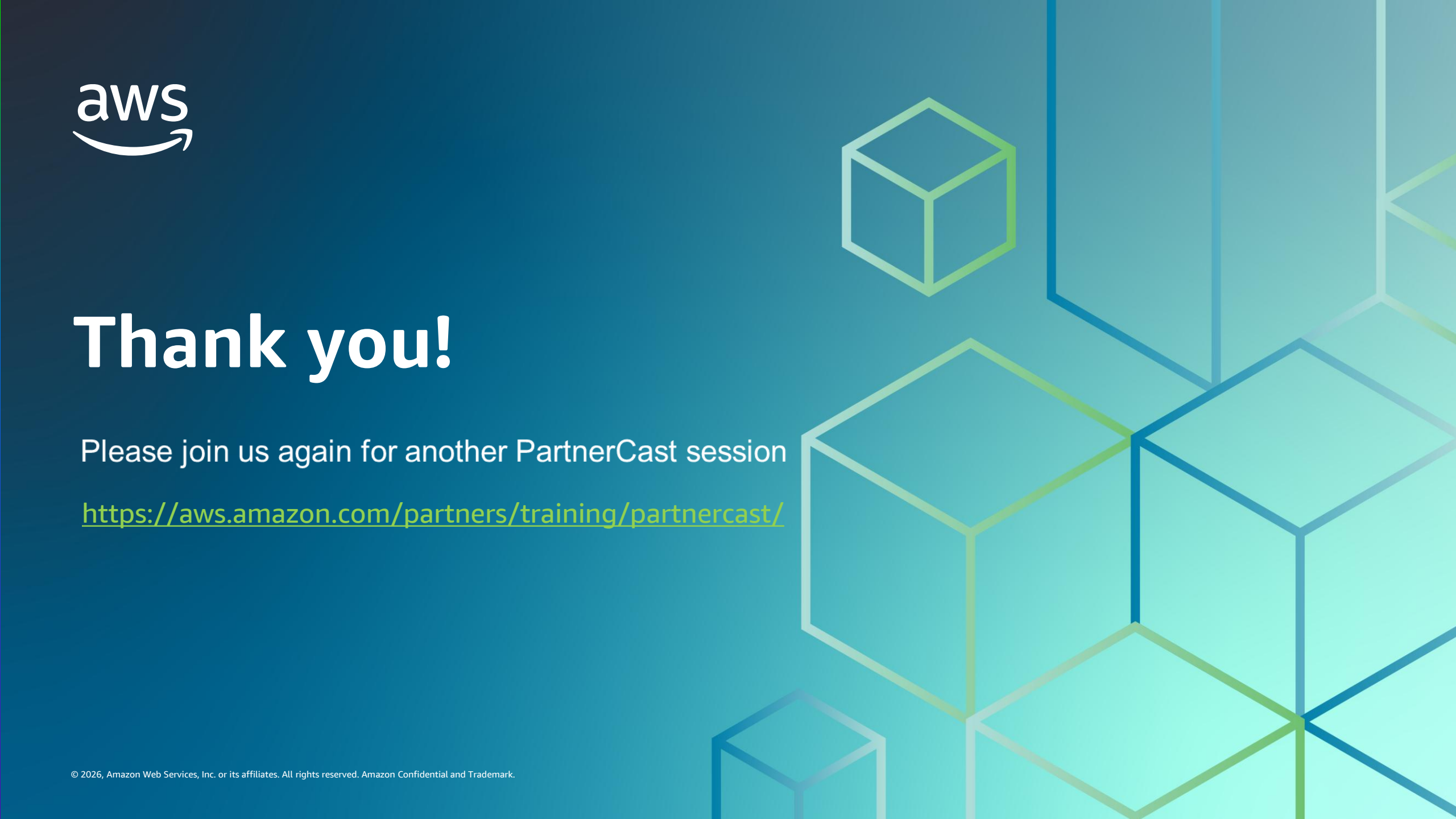
Cloud WANの構成はCloudFormationやCloud WAN内の設定を定義するCNP(Core Network Policy)でIaC化可能。

まとめ

- AWSバックボーンネットワークを活用することで、AWSグローバルインフラストラクチャをオンプレミスネットワークの延長として利用できます。お客様のWAN環境においても、クラウドならではの高い俊敏性を得ることが可能です。

- AWS Cloud WANは、グローバルに展開されたオンプレミス拠点間や、AWS環境へのネットワーク接続を迅速に提供します。豊富なアタッチメントタイプをサポートしており、拠点間およびVPC間のグローバルルーティングが可能です。また、ネットワーク全体を一元的なダッシュボードからポリシーベースで定義・監視できるため、運用の負担を大幅に軽減します。またIaC化することで手動操作のエラー回避や迅速なデプロイ、管理の効率化を実現できます。

- AWS Cloud WANは、SASEやSD-WAN等のパートナーソリューションと統合可能なクラウドネイティブな基盤を提供します。これにより、一貫したガバナンスを保ちつつ、セキュアなグローバルネットワークの迅速な展開を実現します。



Thank you!

Please join us again for another PartnerCast session

https://aws.amazon.com/partners/training/partnercast/